

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**Jerry Allen, Dean Armstrong, Eric Barber,
Patricia Baxter, Jaclyn Belland, Douglas
Benz, Michael Bishop, Darlene Brown, Kody
Campbell, Bridget Craney, Linda DeVore,
Trevor Dorsey, Eileen Doten, Nancy Dubin,
Abby Elliott, Kayla Ferrel, Terry Ford,
Jasmine Guess, Vanuel Harris, Zacariah
Hildenbrand, Robert Hunt, Tammy Jett,
Joseph Creed Kelly, Manuel Lucero,
Kathleen Lyons, Tanya Mack, Darin
Marion, Christina Martell, Carlos Martinho,
Craig Maxwell, Mary Hexter Money Penny,
Gerald Muhammad, Glenntavius Nolan,
Wayne Norris, Kyle Olson, Mel Orchard III,
Bruce Pascal, Mercedes Pillette, Alexandra
Santana, Miche' Sharpe, Andrew Sheppe,
Amie Smith, Mike Spicer, Mildred Sutton,
Katherine Timmons, Lisa Tyree, Nicole
Walker, Carolyn White, David White,
Robert Wickens, Jennifer Wise, and Kyoko
Yamamoto,**

Plaintiffs,

v.

EQUIFAX, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

I.	INTRODUCTION	9
II.	JURISDICTION AND VENUE	12
III.	PARTIES	14
	A. Plaintiffs.	14
	B. Defendant	48
IV.	FACTS	49
	A. Equifax, As One of Three Major Credit Reporting Companies, Obtains and Uses Sensitive Personal and Financial Information from Millions of Consumers	49
	B. Equifax Expands Into New Business Areas, But Fails to Improve Data Safeguards	50
	C. The Equifax Data Breach	56
	D. Equifax Fumbles When It Finally Alerts Customers	60
	E. Equifax Starts Laying Blame Elsewhere.....	66
	F. Equifax Attempts to Leverage Its Negligence to Benefit Financially from the Harm It Caused.....	70
	G. The Lasting Impact of Equifax’s Negligence is Just Starting to be Felt	71
V.	CLASS ALLEGATIONS	79
VI.	CLAIMS ALLEGED ON BEHALF OF THE NATIONWIDE CLASS	84
	FIRST CAUSE OF ACTION: FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681, <i>et seq.</i>	84
	SECOND CAUSE OF ACTION: NEGLIGENCE	87
	THIRD CAUSE OF ACTION: NEGLIGENCE <i>PER SE</i>	94
	FOURTH CAUSE OF ACTION: BAILMENT	97

FIFTH CAUSE OF ACTION: UNJUST ENRICHMENT	99
VII. STATE CONSUMER PROTECTION LAWS BROUGHT BY THE STATEWIDE SUBCLASSES BELOW	101
SIXTH CAUSE OF ACTION: ALABAMA DECEPTIVE TRADE PRACTICES ACT, Ala. Code §§8-19-1, <i>et seq.</i>	101
SEVENTH CAUSE OF ACTION:ALASKA CONSUMER PROTECTION ACT, AS §§ 45.50.471, <i>et seq.</i>	104
EIGHTH CAUSE OF ACTION:ARIZONA CONSUMER FRAUD ACT, A.R.S. §§ 44-1521, <i>et seq.</i>	106
NINTH CAUSE OF ACTION:ARKANSAS DECEPTIVE TRADE PRACTICES ACT, A.C.A. §§ 4-88-101, <i>et seq.</i>	110
TENTH CAUSE OF ACTION:CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §§ 17200, <i>et seq.</i>	112
ELEVENTH CAUSE OF ACTION:CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, <i>et seq.</i>	116
TWELFTH CAUSE OF ACTION: COLORADO CONSUMER PROTECTION ACT, Colo. Rev. Stat. §§ 6-1-101, <i>et seq.</i>	118
THIRTEENTH CAUSE OF ACTION: CONNECTICUT UNFAIR TRADE PRACTICES ACT, C.G.S. §§ 42-110a <i>et seq.</i>	122
FOURTEENTH CAUSE OF ACTION:VIOLATION OF THE DELAWARE CONSUMER FRAUD ACT, 6 Del. Code §§ 2513, <i>et</i> <i>seq.</i>	125
FIFTEENTH CAUSE OF ACTION: DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT, D.C. Code §§ 28-3904, <i>et seq.</i>	128
SIXTEENTH CAUSE OF ACTION: FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, <i>et</i> <i>seq.</i>	132

SEVENTEENTH CAUSE OF ACTION: GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Ga. Code Ann. §§ 10-1- 370, <i>et seq.</i>	135
EIGHTEENTH CAUSE OF ACTION: HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION STATUTE, Haw. Rev. Stat. §§ 480-1, <i>et seq.</i>	141
NINETEENTH CAUSE OF ACTION: IDAHO CONSUMER PROTECTION ACT, Idaho Code §§ 48-601, <i>et seq.</i>	145
TWENTIETH CAUSE OF ACTION: ILLINOIS CONSUMER FRAUD ACT, 815 Ill. Comp. Stat. §§ 505/1, <i>et seq.</i> (Asserted by the Illinois Subclass).....	147
TWENTY-FIRST CAUSE OF ACTION: ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 Ill. Comp. Stat. §§ 510/2, <i>et seq.</i>	150
TWENTY-SECOND CAUSE OF ACTION: IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT, Iowa Code § 714H.....	151
TWENTY-THIRD CAUSE OF ACTION: KANSAS CONSUMER PROTECTION ACT, K.S.A. §§ 50-623, <i>et seq.</i>	153
TWENTY-FOURTH CAUSE OF ACTION: KENTUCKY CONSUMER PROTECTION ACT, Ky. Rev. Stat. §§ 367.110, <i>et seq.</i>	156
TWENTY-FIFTH CAUSE OF ACTION: LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, La Rev. Stat. Ann. §§ 51:1401, <i>et seq.</i>	159
TWENTY-SIXTH CAUSE OF ACTION: MAINE UNFAIR TRADE PRACTICES ACT, 5 Me. Rev. Stat. §§ 205, 213, <i>et seq.</i>	164
TWENTY-SEVENTH CAUSE OF ACTION: MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT, 10 Me. Rev. Stat. §§ 1212, <i>et seq.</i>	168

TWENTY-EIGHTH CAUSE OF ACTION: MARYLAND CONSUMER PROTECTION ACT, Md. Code Ann., Com. Law §§ 13-301, <i>et seq.</i>	169
TWENTY-NINTH CAUSE OF ACTION: MASSACHUSETTS CONSUMER PROTECTION ACT, Mass. Gen. Laws Ann. Ch. 93A, §§ 1, <i>et seq.</i>	173
THIRTIETH CAUSE OF ACTION: MICHIGAN CONSUMER PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.903, <i>et seq.</i>	176
THIRTY-FIRST CAUSE OF ACTION: MINNESOTA CONSUMER FRAUD ACT, Minn. Stat. §§ 325F.68, <i>et seq.</i> and Minn. Stat. §§ 8.31, <i>et seq.</i>	180
THIRTY-SECOND CAUSE OF ACTION: MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Minn. Stat. §§ 325D.43, <i>et seq.</i>	183
THIRTY-THIRD CAUSE OF ACTION: MISSOURI MERCHANDISE PRACTICES ACT, Mo. Rev. Stat. §§ 407.010, <i>et</i> <i>seq.</i>	186
THIRTY-FOURTH CAUSE OF ACTION: MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, MCA §§ 30-14-101, <i>et seq.</i>	190
THIRTY-FIFTH CAUSE OF ACTION: NEBRASKA CONSUMER PROTECTION ACT, Neb. Rev. Stat. §§ 59-1601, <i>et seq.</i>	193
THIRTY-SIXTH CAUSE OF ACTION: NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Neb. Rev. Stat. §§ 87-301, <i>et seq.</i>	197
THIRTY-SEVENTH CAUSE OF ACTION: NEVADA DECEPTIVE TRADE PRACTICES ACT, Nev. Rev. Stat. Ann. §§ 598.0915, <i>et</i> <i>seq.</i>	200
THIRTY-EIGHTH CAUSE OF ACTION: NEW HAMPSHIRE CONSUMER PROTECTION ACT, N.H.R.S.A. §§ 358-A, <i>et seq.</i>	203

THIRTY-NINTH CAUSE OF ACTION: NEW JERSEY CONSUMER FRAUD ACT, N.J. Stat. Ann. §§ 56:8-1, <i>et seq.</i>	206
FORTIETH CAUSE OF ACTION: NEW MEXICO UNFAIR PRACTICES ACT, N.M. Stat. Ann. §§ 57-12-2, <i>et seq.</i>	210
FORTY-FIRST CAUSE OF ACTION: NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, <i>et seq.</i>	213
FORTY-SECOND CAUSE OF ACTION:NORTH CAROLINA UNFAIR TRADE PRACTICES ACT, N.C. Gen. Stat. Ann. §§ 75- 1.1, <i>et seq.</i>	216
FORTY-THIRD CAUSE OF ACTION: NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT, N.D. Cent. Code §§ 51-10-01, <i>et seq.</i>	220
FORTY-FOURTH CAUSE OF ACTION: OHIO CONSUMER SALES PRACTICES ACT, Ohio Rev. Code §§ 1345.01, <i>et seq.</i>	224
FORTY-FIFTH CAUSE OF ACTION: OHIO DECEPTIVE TRADE PRACTICES ACT, Ohio Rev. Code §§ 4165.01, <i>et seq.</i>	227
FORTY-SIXTH CAUSE OF ACTION:OKLAHOMA CONSUMER PROTECTION ACT, Okla. Stat. Tit. 15, §§ 751, <i>et seq.</i>	230
FORTY-SEVENTH CAUSE OF ACTION:OREGON UNLAWFUL TRADE PRACTICES ACT, Or. Rev. Stat. §§ 646.608, <i>et seq.</i>	234
FORTY-EIGHTH CAUSE OF ACTION:PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, <i>et seq.</i>	237
FORTY-NINTH CAUSE OF ACTION:RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT, R.I. Gen. Laws §§ 6-13.1, <i>et seq.</i>	241
FIFTIETH CAUSE OF ACTION:SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT, S.C. Code Ann. §§ 39-5-10, <i>et seq.</i>	245

FIFTY-FIRST CAUSE OF ACTION: SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT, S.D. Codified Laws §§ 37-24-1, <i>et seq.</i>	249
FIFTY-SECOND CAUSE OF ACTION: TENNESSEE CONSUMER PROTECTION ACT, Tenn. Code Ann. §§ 47-18-101, <i>et seq.</i>	253
FIFTY-THIRD CAUSE OF ACTION: UTAH CONSUMER SALES PRACTICES ACT, Utah Code §§ 13-11-1, <i>et seq.</i>	256
FIFTY-FOURTH CAUSE OF ACTION: VERMONT CONSUMER FRAUD ACT, Vt. Stat. Ann. Tit. 9, §§ 2451, <i>et seq.</i>	260
FIFTY-FIFTH CAUSE OF ACTION: VIRGINIA CONSUMER PROTECTION ACT, Va. Code Ann. §§ 59.1-196, <i>et seq.</i>	263
FIFTY-SIXTH CAUSE OF ACTION: WASHINGTON CONSUMER PROTECTION ACT, Wash. Rev. Code Ann. §§ 19.86.020, <i>et seq.</i>	267
FIFTY-SEVENTH CAUSE OF ACTION: WISCONSIN DECEPTIVE TRADE PRACTICES ACT, Wis. Stat. § 100.18	270
FIFTY-EIGHTH CAUSE OF ACTION: WYOMING CONSUMER PROTECTION ACT, Wyo. Stat. Ann. §§ 40-12-101, <i>et seq.</i>	274
VIII. STATE DATA BREACH STATUTES BROUGHT BY THE STATEWIDE SUBCLASSES BELOW	276
FIFTY-NINTH CAUSE OF ACTION: PERSONAL INFORMATION PROTECTION ACT, Alaska Stat. §§ 45.48.010, <i>et seq.</i>	276
SIXTIETH CAUSE OF ACTION: CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80, <i>et seq.</i>	278
SIXTY-FIRST CAUSE OF ACTION: COLORADO SECURITY BREACH NOTIFICATION ACT, Colo. Rev. Stat. Ann. §§ 6-1-716, <i>et seq.</i>	281
SIXTY-SECOND CAUSE OF ACTION: DELAWARE COMPUTER SECURITY BREACH ACT, 6 Del. Code Ann. §§ 12B-102, <i>et seq.</i>	282

SIXTY-THIRD CAUSE OF ACTION: DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT, D.C. Code §§ 28-3851, <i>et seq.</i>	284
SIXTY-FOURTH CAUSE OF ACTION: GEORGIA SECURITY BREACH NOTIFICATION ACT, Ga. Code Ann. §§ 10-1-912, <i>et</i> <i>seq.</i>	285
SIXTY-FIFTH CAUSE OF ACTION: HAWAII SECURITY BREACH NOTIFICATION ACT, Haw. Rev. Stat. §§ 487N-1, <i>et seq.</i>	286
SIXTY-SIXTH CAUSE OF ACTION: PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, Iowa Code Ann. §§ 715C.2, <i>et seq.</i>	288
SIXTY-SEVENTH CAUSE OF ACTION: Kan. Stat. Ann. §§ 50- 7a02(a), <i>et seq.</i>	290
SIXTY-EIGHTH CAUSE OF ACTION: KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT, Ky. Rev. Stat. Ann. §§ 365.732, <i>et seq.</i>	291
SIXTY-NINTH CAUSE OF ACTION: La. Rev. Stat. Ann. §§ 51:3074(A), <i>et seq.</i>	293
SEVENTIETH CAUSE OF ACTION: MARYLAND PERSONAL INFORMATION PROTECTION ACT, Md. Comm. Code §§ 14- 3501, <i>et seq.</i>	294
SEVENTY-FIRST CAUSE OF ACTION: MARYLAND'S SOCIAL SECURITY NUMBER PRIVACY ACT, Md. Comm. Code §§ 14- 3401, <i>et seq.</i>	297
SEVENTY-SECOND CAUSE OF ACTION: MICHIGAN IDENTITY THEFT PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.72, <i>et seq.</i>	298
SEVENTY-THIRD CAUSE OF ACTION: N.H. Rev. Stat. Ann. §§ 359-C:20(I))(a), <i>et seq.</i>	300

SEVENTY-FOURTH CAUSE OF ACTION: NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J. Stat. Ann. §§ 56:8-163, <i>et seq.</i>	301
SEVENTY-FIFTH CAUSE OF ACTION: NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. Gen. Stat. Art. 2A §§ 75-60, <i>et seq.</i>	303
SEVENTY-SIXTH CAUSE OF ACTION: OREGON CONSUMER IDENTITY THEFT PROTECTION ACT, Or. Rev. Stat. Ann. §§ 646a.604(1), <i>et seq.</i>	305
SEVENTY-SEVENTH CAUSE OF ACTION: SOUTH CAROLINA DATA BREACH SECURITY ACT, S.C. Code Ann. §§ 39-1-90, <i>et</i> <i>seq.</i>	307
SEVENTY-EIGHTH CAUSE OF ACTION: TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, Tenn. Code Ann. §§ 47-18-2107, <i>et seq.</i>	308
SEVENTY-NINTH CAUSE OF ACTION: VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT Va. Code. Ann. §§ 18.2-186.6, <i>et seq.</i>	310
EIGHTIETH CAUSE OF ACTION: WASHINGTON DATA BREACH NOTICE ACT, Wash. Rev. Code Ann. §§ 19.255.010, <i>et</i> <i>seq.</i>	311
EIGHTY-FIRST CAUSE OF ACTION: Wis. Stat. Ann. §§ 134.98(2), <i>et seq.</i>	313
EIGHTY-SECOND CAUSE OF ACTION: Wyo. Stat. Ann. §§ 40- 12-502(a), <i>et seq.</i>	315
EIGHTY-THIRD CAUSE OF ACTION: DECLARATORY AND INJUNCTIVE RELIEF	316
REQUEST FOR RELIEF	319
DEMAND FOR JURY TRIAL	320

Plaintiffs Jerry Allen, Dean Armstrong, Eric Barber, Patricia Baxter, Jaclyn Belland, Douglas Benz, Michael Bishop, Darlene Brown, Kody Campbell, Bridget Craney, Linda DeVore, Trevor Dorsey, Eileen Doten, Nancy Dubin, Abby Elliott, Kayla Ferrel, Terry Ford, Jasmine Guess, Vanuel Harris, Zacariah Hildenbrand, Robert Hunt, Tammy Jett, Joseph Creed Kelly, Manuel Lucero, Kathleen Lyons, Tanya Mack, Darin Marion, Christina Martell, Carlos Martinho, Craig Maxwell, Mary Hexter Moneypenny, Gerald Muhammad, Glenntavius Nolan, Wayne Norris, Kyle Olson, Mel Orchard III, Bruce Pascal, Mercedes Pillette, Alexandra Santana, Miche' Sharpe, Andrew Sheppe, Amie Smith, Mike Spicer, Mildred Sutton, Katherine Timmons, Lisa Tyree, Nicole Walker, Carolyn White, David White, Robert Wickens, Jennifer Wise, and Kyoko Yamamoto (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" and "Subclasses," as more fully defined below), bring this action against Equifax, Inc. ("Equifax"), to recover monetary damages, injunctive relief, and other remedies for violations of federal and state statutes and the common law.

I. INTRODUCTION

1. This case concerns the largest data breach involving personal and financial information in American history. Equifax, one of the three major credit

reporting companies used by thousands of businesses to assess the credit worthiness of customers and prospective customers, failed spectacularly in protecting that data. Its misfeasance has allowed thieves to steal the valuable personal identification and financial information (“Personal Information” or “PII”) of more than 145.5 million Americans—nearly half of the United States’ population (the “Equifax Data Breach”). This data permits thieves to create fake identities, fraudulently obtain loans, swipe tax refunds, and destroy the customer’s credit worthiness—the very thing Equifax existed to assess.

2. Compounding this massive breach is Equifax’s egregious cybersecurity failings before, during, and after the breach. While each day brings further details of Equifax’s derelictions, the current tally of its misdeeds includes:

- a. Failing to employ a security patch provided by a software maker;
- b. Not recognizing the breach for more than three months;
- c. Not implementing security measures after the breach to prevent further attacks;
- d. Not informing the public of the breach for more than a month, thus preventing consumers from timely acting to freeze their credit

and/or take other measures to protect themselves from the consequences of the breach;

e. During the silence, several top executives selling off \$1.8 million in stock;

f. Finally alerting customers using confusing emails and notices regarding whose data was compromised;

g. Creating a monitoring service with conflicting messages as to whether the arbitration clause mentioned in the terms of service for the website would apply to consumers taking advantage of the service, thereby using a crisis of its own making to deny consumers their Seventh Amendment rights;

h. Sending customers the wrong link to have their credit frozen; and

i. Allowing hackers to access vulnerable code on its website, which prompted consumers to download a fraudulent software update, further exposing their information to bad actors.

3. Equifax has made billions as a credit reporting company that American consumers often do not select, but whose banks, mortgage companies, auto lenders, landlords, and others use to assess their credit. Millions of Americans

unwittingly trusted Equifax to safeguard their critically sensitive and important personal and financial information. But Equifax failed to protect that data and has inspired little confidence in consumers that its free credit monitoring services will fare any better.

4. Herein, Plaintiffs, individually and on behalf of the members of the Class and Subclasses they seek to represent (including for each of the fifty states and the District of Columbia), bring this action against Equifax. Plaintiffs assert claims for themselves and on behalf of a nationwide class of consumers for Equifax's violation of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681, *et seq.*, negligence, negligence *per se*, bailment, and unjust enrichment, and, for themselves and on behalf of state-specific subclasses, for Equifax's violation of state consumer protection and/or privacy laws. Plaintiffs seek monetary damages, declaratory and injunctive relief, and other remedies for violations of federal and state statutes and the common law.

II. JURISDICTION AND VENUE

5. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiffs and the other Class members assert that Equifax violated the FCRA and therefore Plaintiffs' and Class members' claims arise under the laws of the United States.

6. In addition, this Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action, including claims asserted on behalf of a nationwide class and multiple state classes, filed under Rule 23 of the Federal Rules of Civil Procedure; there are likely millions of proposed Class members; the aggregate amount in controversy exceeds the jurisdictional amount of \$5,000,000.00; and Equifax is a citizen of a State different from that of at least one Plaintiff. This Court also has subject-matter jurisdiction over Plaintiffs' and Class members' claims pursuant to 28 U.S.C. § 1367(a).

7. Venue is proper in this District under 28 U.S.C. § 1391 (a)–(d) because, *inter alia*, Equifax's principal place of business is located in the District, substantial parts of the events or omissions giving rise to the claim occurred in the District, and/or a substantial part of property that is the subject of the action is situated in the District. A substantial part of Plaintiffs' personal and financial information and activities that Equifax collected, obtained, maintained, and allowed to be accessed without authorization during the data breach, occurred in or was found in the District. And, a significant part of the risk of harm that Plaintiffs now face through Equifax's wrongful conduct is present in this District. Venue is also proper in the Atlanta Division because Equifax is located here.

III. PARTIES

A. Plaintiffs.

ALABAMA

8. Vanuel Harris is a resident of the State of Alabama. Upon information and belief, Mr. Harris's Social Security number and other personally identifying information were exposed by Equifax. Mr. Harris first learned of the breach on or about October 11, 2017. Concerned his information may have been compromised, Mr. Harris went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Harris's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Harris has experienced fraud, as false loans have been opened in his name. In addition, Mr. Harris paid out of pocket for a credit freeze and credit monitoring as a result of the Equifax breach. Also as a result of the Equifax breach, Mr. Harris has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

ALASKA

9. Michael Bishop is a resident of the State of Alaska. Upon information and belief, Mr. Bishop's Social Security number and other personally identifying information were exposed by Equifax. Mr. Bishop first learned of the breach after

Equifax disclosed the breach on September 7, 2017. Concerned his information may have been compromised, Mr. Bishop went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Bishop's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Bishop has experienced fraud, as unauthorized purchases have been made using his payment card. In addition, Mr. Bishop paid out of pocket for a credit freeze and credit monitoring services as a result of the Equifax breach. As a result of the Equifax breach, Mr. Bishop has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

ARIZONA

10. Zacariah Hildenbrand is a resident of the State of Arizona. Upon information and belief, Mr. Hildenbrand's Social Security number and other personally identifying information were exposed by Equifax. Mr. Hildenbrand first learned of the breach on or about September 9, 2017. Concerned his information may have been compromised, Mr. Hildenbrand went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr.

Hildenbrand's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Hildenbrand has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

ARKANSAS

11. Jerry Allen is a resident of the State of Arkansas. Upon information and belief, Mr. Allen's Social Security number and other personally identifying information were exposed by Equifax. Mr. Allen first learned of the breach on or about September 7, 2017. Concerned his information may have been compromised, Mr. Allen went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Allen's information was in fact exposed as a result of Equifax's massive data breach. Creditors have been contacting Mr. Allen about loans for which he has not applied. Furthermore, as a result of the Equifax breach, Mr. Allen has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

CALIFORNIA

12. Miche' Sharpe is a resident of the State of California. Upon information and belief, Ms. Sharpe's Social Security number and other personally

identifying information were exposed by Equifax. Ms. Sharpe first learned of the breach after Equifax disclosed the breach on September 7, 2017. Concerned her information may have been compromised, Ms. Sharpe went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Sharpe's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Ms. Sharpe has experienced fraud, as someone opened multiple accounts in her name. In addition, Ms. Sharpe paid out of pocket for credit monitoring services as a result of this fraud. As a result of the Equifax breach, Ms. Sharpe has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

COLORADO

13. Gerald Muhammad is a resident of the State of Colorado. Upon information and belief, Mr. Muhammad's Social Security number and other personally identifying information were exposed by Equifax. Mr. Muhammad first learned of the breach on or about September 27, 2017. Concerned his information may have been compromised, Mr. Muhammad went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr.

Muhammad's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Muhammad has experienced fraud, as unauthorized purchases have been made using his bank card and credit cards have been applied for in his name. Also as a result of the Equifax data breach, Mr. Muhammad has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

CONNECTICUT

14. Linda DeVore is a resident of the State of Connecticut. Upon information and belief, Ms. DeVore's Social Security number and other personally identifying information was exposed by Equifax. Ms. DeVore first learned of the breach on or about September 20, 2017. Concerned her information may have been compromised, Ms. DeVore went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. DeVore's information was in fact exposed in Equifax's massive data breach. As a result of the Equifax breach, Ms. DeVore has experienced fraud, as someone appears to have opened a credit card in her name and has made multiple attempts to purchase items with that card. As a result of the Equifax breach, Ms. DeVore has spend numerous hours monitoring her accounts and addressing issues arising from the

Equifax Data Breach.

DELAWARE

15. Alexandra Santana is a resident of the State of Delaware. Upon information and belief, Ms. Santana's Social Security number and other personally identifying information were exposed by Equifax. Ms. Santana first learned of the breach on or about October 9, 2017. Concerned her information may have been compromised, Ms. Santana went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Santana's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Santana has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

DISTRICT OF COLUMBIA

16. Joseph Creed Kelly is a resident of the District of Columbia. Upon information and belief, Mr. Kelly's Social Security number and other personally identifying information were exposed by Equifax. Mr. Kelly first learned of the breach on or about September 11, 2017. Concerned his information may have been compromised, Mr. Kelly went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information

was exposed. The response from the website indicated that Mr. Kelly's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Kelly has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

FLORIDA

17. Trevor Dorsey is a resident of the State of Florida. Upon information and belief, Mr. Dorsey's Social Security number and other personally identifying information were exposed by Equifax. Mr. Dorsey first learned of the breach on or about September 21, 2017. Concerned his information may have been compromised, Mr. Dorsey verified through Equifax that his information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Dorsey has experienced fraud, as unauthorized credit cards and loans have been applied for in his name. Also as a result of the Equifax breach, Mr. Dorsey has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

GEORGIA

18. Robert Hunt is a resident of the State of Georgia. Upon information and belief, Mr. Hunt's Social Security number and other personally identifying information were exposed by Equifax. Mr. Hunt first learned of the breach on or

about September 18, 2017. Concerned his information may have been compromised, Mr. Hunt went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Hunt's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Hunt has experienced fraud, as unauthorized mortgages and loans have been applied for in his name. Also as a result of the Equifax breach, Mr. Hunt has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

HAWAII

19. Bruce Pascal is a resident of the State of Hawaii. Upon information and belief, Mr. Pascal's Social Security number and other personally identifying information was exposed by Equifax. Mr. Pascal first learned of the breach on the news. Concerned his information may have been compromised, Mr. Pascal went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Pascal's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Pascal has spent numerous hours monitoring his accounts and addressing issues arising from

the Equifax Data Breach

IDAHO

20. Eileen Doten is a resident of the State of Idaho. Upon information and belief, Ms. Doten's Social Security number and other personally identifying information were exposed by Equifax. Ms. Doten first learned of the breach on the news. Concerned her information may have been compromised, Ms. Doten went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Doten's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Doten has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

ILLINOIS

21. Douglas Benz is a resident of the State of Illinois. Upon information and belief, Mr. Benz's Social Security number and other personally identifying information were exposed by Equifax. Mr. Benz first learned of the breach after Equifax disclosed the breach on September 7, 2017. Concerned his information may have been compromised, Mr. Benz went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his

information was exposed. The response from the website indicated that Mr. Benz's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Benz has experienced fraud, as someone has attempted to open multiple credit accounts in his name using his social security number and date of birth. As a result of the Equifax breach, Mr. Benz has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach, including filing a police report.

INDIANA

22. Tammy Jett is a resident of the State of Indiana. Upon information and belief, Ms. Jett's Social Security number and other personally identifying information were exposed by Equifax. Ms. Jett first learned of the breach on or about September 8, 2017. Concerned her information may have been compromised, Ms. Jett went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Jett's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Jett has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

IOWA

23. Glenntavius Nolan is a resident of the State of Iowa. Upon information and belief, Mr. Nolan Social Security number and other personally identifying information were exposed by Equifax. Mr. Nolan first learned of the breach on or about September 18, 2017. Concerned his information may have been compromised, Mr. Nolan went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Nolan's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Nolan has experienced fraud, as there have been unauthorized charges made on his credit card. Also as a result of the Equifax breach, Mr. Nolan has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

KANSAS

24. Amie Smith is a resident of the State of Kansas. Upon information and belief, Ms. Smith's Social Security number and other personally identifying information were exposed by Equifax. Ms. Smith first learned of the breach after Equifax disclosed the breach on September 7, 2017. Concerned her information may have been compromised, Ms. Smith went to Equifax's emergency response

website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Smith's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Ms. Smith has experienced fraud, as someone used her Personal Information to open a fraudulent cellular telephone account. In addition, Ms. Smith paid out of pocket for a credit freeze and credit monitoring following the Equifax breach. As a result of the Equifax breach, Ms. Smith has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach, including filing a police report.

KENTUCKY

25. Mary Hexter Moneypenny is a disabled senior citizen and resident of the State of Kentucky. Upon information and belief, Ms. Moneypenny's Social Security number and other personally identifying information were exposed by Equifax. Ms. Moneypenny first learned of the breach on or about September 11, 2017. Concerned her information may have been compromised, Ms. Moneypenny went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Moneypenny's information was in fact exposed in Equifax's massive data breach. As a result of the Equifax breach, Ms.

Moneypenny has experienced fraud, as fraudulent charges have appeared on her credit card. As a result of the Equifax breach, Ms. Moneypenny has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

LOUISIANA

26. Jasmine Guess is a resident of the State of Louisiana. Upon information and belief, Ms. Guess's Social Security number and other personally identifying information were exposed by Equifax. After learning of the data breach on or about September 2017, Ms. Guess went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Ms. Guess's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Ms. Guess has experienced fraud, including having fraudulent insurance claims filed in her name through in May and June 2017. As a result of the Equifax breach, Ms. Guess has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

MAINE

27. Kathleen Lyons is a resident of the State of Maine. Upon information

and belief, Ms. Lyons's Social Security number and other personally identifying information were exposed by Equifax. Ms. Lyons first learned of the breach on or about October 4, 2017. Concerned her information may have been compromised, Ms. Lyons went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Lyons's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Lyons has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

MARYLAND

28. Lisa Tyree is a resident of the State of Maryland. Upon information and belief, Ms. Tyree's Social Security number and other personally identifying information were exposed by Equifax. Ms. Tyree first learned of the breach from a news alert sent to her cell phone. Concerned her information may have been compromised, Ms. Tyree went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Tyree's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Tyree has spent numerous hours monitoring her

accounts and addressing issues arising from the Equifax Data Breach.

MASSACHUSETTS

29. Jaclyn Belland is a resident of the Commonwealth of Massachusetts. Upon information and belief, Ms. Belland's Social Security number and other personally identifying information were exposed by Equifax. Ms. Belland first learned of the breach on or about September 8, 2017. Concerned her information may have been compromised, Ms. Belland went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Belland's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Ms. Belland has experienced fraud, as there have been unauthorized charges made on her credit card. Also as a result of the Equifax breach, Ms. Belland has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

MICHIGAN

30. Nicole Walker is a resident of the State of Michigan. Upon information and belief, Ms. Walker's Social Security number and other personally identifying information were exposed by Equifax. Ms. Walker first learned of the breach on or about September 25, 2017. Concerned her information may have been

compromised, Ms. Walker went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Walker's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Walker has experienced fraud, as she has suffered identity theft. Also as a result of the Equifax breach, Ms. Walker has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

MINNESOTA

31. Mike Spicer is a resident of the State of Minnesota. Upon information and belief, Mr. Spicer's Social Security number and other personally identifying information were exposed by Equifax. Mr. Spicer first learned of the breach on or about September 25, 2017. Concerned his information may have been compromised, Mr. Spicer went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Spicer's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Spicer has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

MISSISSIPPI

32. Manuel Lucero is a resident of the State of Mississippi. Upon information and belief, Mr. Lucero's Social Security number and other personally identifying information were exposed by Equifax. Mr. Lucero first learned of the breach on or about September 29, 2017. Concerned his information may have been compromised, Mr. Lucero went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Lucero's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Lucero has experienced fraud as unauthorized student loans have been applied for using his name. As a result of the Equifax breach, Mr. Lucero has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

MISSOURI

33. Kayla Ferrel is a resident of the State of Missouri. Upon information and belief, Ms. Ferrel's Social Security number and other personally identifying information were exposed by Equifax. Ms. Ferrel first learned of the breach on or about September 11, 2017. Concerned her information may have been compromised, Ms. Ferrel went to Equifax's emergency response website,

trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Ferrel's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Ferrel has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

MONTANA

34. Terry Ford is a resident of the State of Montana. Upon information and belief, Mr. Ford's Social Security number and other personally identifying information were exposed by Equifax. Mr. Ford first learned of the breach on or about October 6, 2017. Concerned his information may have been compromised, Mr. Ford went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Ford's information was in fact exposed as a result of Equifax's massive data breach. As a result of the breach, Mr. Ford has experienced fraud, as unauthorized accounts have been opened in his name. Also as a result of the Equifax breach, Mr. Ford has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

NEBRASKA

35. Eric Barber is a resident of the State of Nebraska. Upon information and belief, Mr. Barber's Social Security number and other personally identifying information were exposed by Equifax. Mr. Barber first learned of the breach on or about October 2, 2017. Concerned his information may have been compromised, Mr. Barber went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Barber's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Barber has experienced fraud, as several credit cards have been opened in his name. Also as a result of the Equifax breach, Mr. Barber has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

NEVADA

36. Katherine Timmons is a resident of the State of Nevada. Upon information and belief, Ms. Timmons's Social Security number and other personally identifying information were exposed by Equifax. Ms. Timmons first learned of the breach on or about October 5, 2017. Concerned her information may have been compromised, Ms. Timmons went to Equifax's emergency response

website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Timmons's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Timmons has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

NEW HAMPSHIRE

37. Andrew Sheppe is a resident of the State of New Hampshire. Upon information and belief, Mr. Sheppe's Social Security number and other personally identifying information were exposed by Equifax. Mr. Sheppe first learned of the breach on September 14, 2017. Concerned that his information may have been compromised, Mr. Sheppe's wife, on behalf of Mr. Sheppe, went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Sheppe's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Sheppe anticipates spending numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

NEW JERSEY

38. Carlos Martinho is a resident of the State of New Jersey. Upon information and belief, Mr. Martinho's Social Security number and other personally identifying information were exposed by Equifax. Mr. Martinho first learned of the breach on or about September 19, 2017. Concerned his information may have been compromised, Mr. Martinho went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Martinho's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Martinho has experienced fraud, as unauthorized charges have been made using his credit card. Also as a result of the Equifax breach, Mr. Martinho has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

NEW MEXICO

39. Dean Armstrong is a resident of the State of New Mexico. Upon information and belief, Mr. Armstrong's Social Security number and other personally identifying information were exposed by Equifax. Mr. Armstrong first learned of the breach after Equifax disclosed the breach on September 7, 2017. Concerned his information may have been compromised, Mr. Armstrong went to

Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Armstrong's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Armstrong has experienced fraud, as someone used his Personal Information to open a fraudulent credit card account. As a result of the Equifax breach, Mr. Armstrong has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

NEW YORK

40. Kyoko Yamamoto is a resident of the State of New York. Upon information and belief, Ms. Yamamoto's Social Security number and other personally identifying information were exposed by Equifax. Ms. Yamamoto first learned of the breach September 8, 2017. Concerned her information may have been compromised, Ms. Yamamoto went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Yamamoto's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Ms. Yamamoto has experienced fraud, as there have been at least two unauthorized charges made on her debit card.

Also as a result of the Equifax breach, Ms. Yamamoto has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

NORTH CAROLINA

41. Plaintiff Nancy Dubin is a resident of the State of North Carolina. Upon information and belief, Ms. Dubin's Social Security number and other personally identifying information were exposed by Equifax. Ms. Dubin first learned of the breach on or about September 15, 2017. Concerned her information may have been compromised, Ms. Dubin went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Dubin's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Ms. Dubin has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

NORTH DAKOTA

42. Christina Martel is a resident of the State of North Dakota. Upon information and belief, Ms. Martell's Social Security number and other personally identifying information were exposed by Equifax. Ms. Martell first learned of the

breach on or about October 11, 2017. Concerned her information may have been compromised, Ms. Martell went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Martell's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Martell has experienced fraud, as unauthorized purchases have been made using her card. Also as a result of the Equifax breach, Ms. Martell has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach

OHIO

43. David White is a resident of the State of Ohio. Upon information and belief, Mr. White's Social Security number and other personally identifying information were exposed by Equifax. Mr. White first learned of the breach on or about September 22, 2017. Concerned his information may have been compromised, Mr. White went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. White's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. White has experienced fraud, as money has

been stolen from his bank account. Also as a result of the Equifax breach, Mr. White has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

OKLAHOMA

44. Darin Marion is a resident of the State of Oklahoma. Upon information and belief, Mr. Marion's Social Security number and other personally identifying information were exposed by Equifax. Mr. Marion first learned of the breach on or about September 18, 2017. Concerned his information may have been compromised, Mr. Marion went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Marion's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Marion has experienced fraud, as unauthorized credit cards have been opened in his name. Also as a result of the Equifax breach, Mr. Marion has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

OREGON

45. Patricia Baxter is a resident of the State of Oregon. Upon information and belief, Ms. Baxter's Social Security number and other personally

identifying information were exposed by Equifax. Ms. Baxter first learned of the breach on or about October 4, 2017. Concerned her information may have been compromised, Ms. Baxter went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Baxter's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Baxter has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

PENNSYLVANIA

46. Mercedes Pillette is a resident of the Commonwealth of Pennsylvania. Upon information and belief, Ms. Pillette's Social Security number and other personally identifying information were exposed by Equifax. Ms. Pillette first learned of the breach on or about September 27, 2017. Concerned her information may have been compromised, Ms. Pillette went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Pillette's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Pillette has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data

Breach.

RHODE ISLAND

47. Darlene Brown is a resident of the State of Rhode Island. Upon information and belief, Ms. Brown's Social Security number and other personally identifying information were exposed by Equifax. Ms. Brown first learned of the breach on or about September 7, 2017. Concerned her information may have been compromised, Ms. Brown went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Brown's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Ms. Brown has experienced fraud, as her debit card was compromised. Also as a result of the Equifax breach, Ms. Brown has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

SOUTH CAROLINA

48. Craig Maxwell is a resident of the State of South Carolina. Upon information and belief, Mr. Maxwell's Social Security number and other personally identifying information were exposed by Equifax. Mr. Maxwell first learned of the breach on or about September 23, 2017. Concerned his information

may have been compromised, Mr. Maxwell went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Maxwell's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Maxwell has experienced fraud, as an unauthorized P.O. Box was opened in his name. Also as a result of the Equifax breach, Mr. Maxwell has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

SOUTH DAKOTA

49. Kody Campbell is a resident of the State of South Dakota. Upon information and belief, Mr. Campbell's Social Security number and other personally identifying information were exposed by Equifax. Mr. Campbell first learned of the breach on or about October 6, 2017. Concerned his information may have been compromised, Mr. Campbell went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Campbell's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Campbell has a mortgage in his name for which he did not apply. Also as a result of the Equifax breach, Mr.

Campbell has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

TENNESSEE

50. Mildred Sutton is a resident of the State of Tennessee. Upon information and belief, Ms. Sutton's Social Security number and other personally identifying information were exposed by Equifax. Ms. Sutton first learned of the breach on or about September 25, 2017. Concerned her information may have been compromised, Ms. Sutton went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Sutton's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Sutton has experienced fraud, as credit cards have been applied for in her name and unauthorized purchases have been made. Also as a result of the Equifax breach, Ms. Sutton has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

TEXAS

51. Wayne Norris is a resident of the State of Texas. Upon information and belief, Mr. Norris's Social Security number and other personally identifying information were exposed by Equifax. Mr. Norris first learned of the breach on or

about September 19, 2017. Concerned his information may have been compromised, Mr. Norris went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Norris's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax Data Breach, Mr. Norris has experienced fraud, as LifeLock notified him that his identity has been stolen. Also as a result of the Equifax breach, Mr. Norris has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

52. Carolyn White is a resident of the State of Texas. Upon information and belief, Ms. White's Social Security number and other personally identifying information were exposed by Equifax. Ms. White first learned of the breach after Equifax disclosed the breach on September 7, 2017. Ms. White was notified by email that her personal information was in fact exposed as a result of Equifax's massive data breach. Ms. White paid out of pocket for credit monitoring services as a result of the Equifax breach. As a result of the Equifax breach, Ms. White has spent time monitoring her accounts and addressing issues arising from the Equifax Data Breach.

UTAH

53. Abby Elliott is a resident of the State of Utah. Upon information and belief, Ms. Elliott's Social Security number and other personally identifying information were exposed by Equifax. Ms. Elliott first learned of the breach on or around September 8, 2017. Concerned her information may have been compromised, Ms. Elliott went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Elliott's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Elliott has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

VERMONT

54. Jennifer Wise is a resident of the State of Vermont. Upon information and belief, Mrs. Wise's Social Security number and other personally identifying information were exposed by Equifax. Mrs. Wise first learned of the breach on or about October 11, 2017. Concerned her information may have been compromised, Mrs. Wise went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Mrs. Wise's information was in fact

exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mrs. Wise has experienced fraud, as she has been getting collection phone calls regarding loans that she never opened. Also as a result of the Equifax breach, Ms. Wise has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

VIRGINIA

55. Bridgette Craney is a resident of the State of Virginia. Upon information and belief, Ms. Craney's Social Security number and other personally identifying information were exposed by Equifax. Ms. Craney first learned of the breach on or about September 14, 2017. Concerned her information may have been compromised by this breach, Ms. Craney went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Craney's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Craney has experienced identity theft and fraud, as multiple fraudulent charges appeared on five of her existing credit card accounts and two new store credit accounts were opened her name without her authorization. As a result of the Equifax breach, Ms. Craney has spent numerous hours completing police reports, monitoring her

accounts and addressing the fraudulent issues arising from the Equifax Data Breach.

WASHINGTON

56. Robert Wickens is a disabled senior citizen and resident of the State of Washington. Upon information and belief, Mr. Wickens' Social Security number and other personally identifying information were exposed by Equifax. Mr. Wickens first learned of the breach on or about September 7, 2017. Concerned his information may have been compromised by this breach, Mr. Wickens went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Wickens' information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Wickens has experienced fraud, as there have been several fraudulent charges on his Social Security debit card account. In addition, Mr. Wickens has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

WEST VIRGINIA

57. Tanya Mack is a resident of the State of West Virginia. Upon information and belief, Ms. Mack's Social Security number and other personally

identifying information were exposed by Equifax. Ms. Mack first learned of the breach on or about September 18, 2017. Concerned her information may have been compromised, Ms. Mack went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Mack's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Ms. Mack has spent numerous hours monitoring her accounts and addressing issues arising from the Equifax Data Breach.

WISCONSIN

58. Kyle Olson is a resident of the State of Wisconsin. Upon information and belief, Mr. Olson's Social Security number and other personally identifying information were exposed by Equifax. Mr. Olson first learned of the breach on or about September 29, 2017. Concerned his information may have been compromised, Mr. Olson went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Olson's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Olson has experienced fraud, as unauthorized purchases have been made using his bank card. Also as a result of the Equifax

breach, Mr. Olson has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

WYOMING

59. Mel C. Orchard III is a resident of the State of Wyoming. Upon information and belief, Mr. Orchard's Social Security number and other personally identifying information were exposed by Equifax. Mr. Orchard first learned of the breach on October 4, 2017. Concerned his information may have been compromised, Mr. Orchard went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Orchard's information was in fact exposed as a result of Equifax's massive data breach. As a result of the Equifax breach, Mr. Orchard has spent numerous hours monitoring his accounts and addressing issues arising from the Equifax Data Breach.

B. Defendant

60. Equifax is a Georgia corporation, with its principal place of business in Atlanta, Georgia. Equifax is subject to the jurisdiction of this Court and may be served with process through its registered agent, Shawn Baldwin, 1550 Peachtree Street, N.W., Atlanta, Georgia, which is located in Fulton County, Georgia.

IV. FACTS

A. Equifax, As One of Three Major Credit Reporting Companies, Obtains and Uses Sensitive Personal and Financial Information from Millions of Consumers

61. Equifax began as an investigation firm in 1899. At that time, it gathered up data on customers paying their bills, so grocers knew which customers were creditworthy.¹

62. Equifax is one of three nationwide credit reporting companies that track and rate the financial history of U.S. consumers, which have been referred to as “linchpins” of the financial system.²

63. Louis Hyman, a consumer-credit historian at Cornell University, explained: “Credit bureaus are the tracks that the [credit] trains run on, and we should make sure those roads and tracks are sound if we’re going to run a whole economy over them.”³

64. Equifax is supplied with data about loans, loan payments and credit cards, as well as information on everything from credit limits and terms to employment history, from child support payments to missed rent and utilities

¹ <https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html?smprod=nytcore-ipad&smid=nytcore-ipad-share> (last accessed October 23, 2017).

² <https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318> (last accessed October 23, 2017).

³ *Id.*

payments. All of this highly sensitive information is then factored into the credit reports that Equifax maintains and provides to financial companies, employers, and other entities that use those reports to make decisions about individuals in a range of areas.

65. Today Equifax organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers.

66. Equifax is publicly traded on the New York Stock Exchange (ticker symbol EFX). In 2016, it generated revenues of \$3.144 billion.

B. Equifax Expands Into New Business Areas, But Fails to Improve Data Safeguards

67. Equifax sells identity and authentication systems, known as “out of wallet” or “OOW” questions. These services can be utilized during initial account setup or password resets to “leverage” information “in most consumers’ credit files to perform a reasonably strong authentication” by asking questions like “What was your address when you were 18?” and “Do you have an auto loan with a monthly payment of \$245?”⁴

68. Of course, these services, too, involve consumers providing Equifax

⁴ <http://www.linkedin.com/pulse/massive-equifax-breach-may-reduce-strength-out-wallet-jeff-schmidt?trk=mp-reader-card> (last accessed October 24, 2017).

with sensitive financial and personal information as part of the consumers paying for, and Equifax providing, such services. In addition to providing services to individual consumers, Equifax also supplies identity verification services to the U.S. Social Security Administration and works with the federal Centers for Medicare and Medicaid Services to verify eligibility for health-insurance subsidies.⁵

69. These services include helping consumers check their Social Security benefits and request replacement Social Security cards, as well as to verify eligibility for subsidies to buy health insurance under the Affordable Care Act.⁶

70. Perhaps no other corporations in the U.S. maintains as much sensitive personal and financial information about consumers as do Equifax and the other two credit reporting companies.

71. Equifax has previously stated that its “partnership will help protect the millions of online transactions the SSA manages annually.”⁷

72. In fact, in recent years, Equifax had made a concerted effort to gain an advantage over other credit reporting companies and “moved to acquire more

⁵ Michael Rapoport & AnnaMaria Andriotis, *Equifax Work for Government Shows Its Broad Reach*, WALL ST. J., Sept. 19, 2017, at B2.

⁶ *Id.*

⁷ *Id.*

databases on Americans and then sell that data,” including “a trove of employment records in large part due to its acquisition of Talx Corp. in 2007” and expanding the number of people for which it had credit reports by paying \$1 billion in 2012 to acquire Computer Science Corp.’s credit services unit, which gave it access to credit files for about 20% of the U.S. population.⁸

73. Equifax has persuaded more than 7,000 employers to hand over salary details for an income verification system that encompasses nearly half of American workers.⁹

74. However, in 2014, Equifax left private encryption keys on its server.¹⁰ This allows anyone who gains access to the server to also gain access to the key, giving them the ability to decrypt the relevant encrypted data into its original form.

75. Equifax also experienced several prior hacking incidents and security vulnerabilities. In 2016 and 2017, cybercriminals exploited vulnerability in an Equifax website to steal W-2 tax data.¹¹ Also in 2016, a security researcher

⁸ *Id.*

⁹ <https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html?smprod=nytcore-ipad&smid=nytcore-ipad-share#story-continues-2> (last accessed October 23, 2017).

¹⁰ <https://twitter.com/briankrebs/status/908722014449520642> (last accessed October 23, 2017).

¹¹ <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html> (last accessed October 23, 2017).

warned Equifax that one of its public-facing websites “displayed several search fields, and anyone –with no authentication whatsoever– could force the site to display the personal data of Equifax’s customers. . . .”¹² It took the company six months to patch that vulnerability.¹³ In February 2017, Equifax disclosed another “technical issue” that compromised credit information belonging to some consumers who used identity-theft protection services from its customer, LifeLock.¹⁴ An additional hack occurred between April 2013 and January 2014 when a hacker accessed credit-report data. In 2015, Equifax exposed consumer data as a result of another “technical error,” this time one that “occurred during a software change.”¹⁵

76. Against the backdrop of its own security issues, Equifax moved to grow beyond just a credit bureau and started selling products to businesses to protect against identity thieves and respond to data breaches:

¹² https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning (last accessed October 27, 2017).

¹³ *Id.*

¹⁴ <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html> (last accessed October 23, 2017).

¹⁵ *Id.*

Member Center Login

About Equifax

Investors

Online Dispute

Contact Us

Search



Think your business is safe from a data breach? Think again.

"More than ever before, your employees and customers are at great risk for identity theft and fraud. Over 165 million data records of U.S. residents have been exposed due to data breaches since January 2005 - Privacy Rights Clearinghouse"

Take Action Today: E-mail us at: breach@equifax.com Or call us at: 1-888-259-2688

Data Breaches are on the rise. Be prepared.

You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events everyday. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market.

Equifax Personal Solutions Capabilities



Notification Capabilities

- Consumer File Updating
- Letter Templates
- Print & Mail Letters



Communication Capabilities

- Event-Specific Hotline



Fulfillment & Customer Care Capabilities

- Fraud Alert Placement
- Customer Care
- Credit Monitoring Product Fulfillment
- Fraud Resolution Assistance
- Credit File Freeze

Experienced help is here.

Equifax can help you prepare with our Equifax Data Breach Response Team -- a dedicated group of professionals that will implement a "data breach response plan" before a breach ever occurs.

Here's how our Response Team provides peace of mind.

We consult with you to create a customized Data Breach Response Plan that will enable you to:

- 1 Quickly inform consumers, employees, and shareholders with pre-defined communications regarding the event and the steps you are taking on their behalf;
- 2 Offer the appropriate level of identity theft protection products based on the risk profile of the data breach (ask about our Data Breach Risk Assessment Matrix);
- 3 Provide a dedicated Call Center to assist breached victims with product related questions after enrollment.
- 4 Place Fraud Alerts on consumers' credit files at all three credit reporting agencies as requested.

Consider what a breach can do.

Knowing that a data breach is a very real possibility, your company needs to be prepared for it.

After all, a breach can have many serious implications:

- Erosion of employee customer trust
- Decline in shareholder value
- Undesirable publicity
- Legal & regulatory liabilities
- Out of budget expenses

Hear what our valued customers are saying about our services.

Thank you both very much for the time and effort you provided to assist us in managing our incident. I was very impressed with your customer focus, ability to change when necessary, and the quality of your services. Thanks again for all your service and support.

A major packaging solutions provider

Become a Valued Customer Today

Get More Information Now

E-mail us at breach@equifax.com or call 1-888-259-2688 to get more information on Equifax Data Breach Solutions and becoming our valued customer. You'll receive a response from a Data Breach Response Team representative within 24 hours on a business day.

You may also view our [Best Demonstrated Practices](#)

White Paper Incident Experience by Industry

- Banking & Finance
- Healthcare
- Insurance
- High Tech & Consulting Services
- Government
- Education
- Manufacturing
- Telecommunications
- Retail
- Hospitality
- Energy/Utilities
- Transportation

Had a small data breach?

Try our family/group plan online.

[Learn More](#)

77. Equifax noted that, “Data breaches are on the rise. Be prepared,” and that “Experienced help is here.”¹⁶

78. Despite these warnings Equifax itself issued, four cyber-risk analysis companies report that Equifax “was behind on basic maintenance of websites that could have been involved in transmitting sensitive consumer information and scored poorly in areas” highly relevant to potential breaches.¹⁷

79. Equifax’s security was rated poorly since at least the beginning of 2017, receiving a FICO enterprise security score around 550 on a scale ranging from 300 to 850. That score comprises assessments of security relating to hardware, network security, and web services.¹⁸

80. In April 2017, cyber-risk analysis firm Cyence assessed the risk of a data breach at Equifax in the next 12 months at 50%, ranking it second-to-last in its peer group of 23 companies.¹⁹

¹⁶ <http://www.equifax.com/help/data-breach-solutions2/> (last accessed October 23, 2017).

¹⁷ http://www.wsj.com/article_email/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947-1MyQjAxMTA3OTIyNjUyMzY5Wj/ (last accessed October 23, 2017).

¹⁸ *Id.*

¹⁹ *Id.*

81. In mid-July 2017, Equifax's FICO enterprise security score hit a low of approximately 475.²⁰

82. Still, Equifax did not bolster its security protocols and practices.

C. The Equifax Data Breach

83. According to a company press release, hackers breached Equifax's data security systems on July 29, 2017.²¹

84. But according to a report prepared by the cybersecurity firm Mandiant, hackers were roaming undetected inside Equifax's computer network since at least March 10, 2017. This is when investigators found the very first evidence of "interaction."²²

85. The March 2017 hack apparently occurred in one of Equifax's servers through a "flaw" in its Apache Struts software.²³

86. In March 2017, tech blogs reported "a string of attacks that have escalated over the past 48 hours [where] hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used

²⁰ *Id.*

²¹ <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832> (last accessed October 23, 2017).

²² http://nypost.com/2017/09/20/hackers-have-been-hiding-in-equifaxs-computer-network-for-months/?utm_campaign=iosapp&utm_source=mail_app (last accessed October 23, 2017).

²³ *Id.*

by banks, government agencies, and large Internet companies.”²⁴

87. On March 7, 2017, three days before the March incident, Apache Software Foundation issued a “patch” to address the flaw, and warned its customers of the risk and the need to implement the patch.²⁵

88. Stories about attempts to batter sites that had yet to apply the patch were available online for any chief information, technology, or security officer competently doing his or her job.²⁶

89. However, Equifax did not utilize this patch, update its software, or otherwise address the vulnerability at that time.²⁷

90. Equifax ignored not only Apache, but also advice from the U.S. Computer Emergency Readiness Team, part of the Department of Homeland Security, which also sent a notice about the same vulnerability.²⁸

91. During his testimony before the House Energy and Commerce

²⁴ <https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/> (last accessed October 23, 2017).

²⁵ <http://www.ajc.com/business/equifax-software-maker-blame-each-other-for-opening-door-hackers/p5wJS5CgTLrmKUL59CTAjM/> (last accessed October 23, 2017).

²⁶ “In-the-wild exploits ramp up against high-impact sites using Apache struts,” Ars Technica, Mar. 14, 2017, available at <https://arstechnica.com/informationtechnology/2017/03/in-the-wild-exploits-ramp-up-against-high-impact-sites-using-apache-struts/> (last accessed October 23, 2017).

²⁷ <http://fortune.com/2017/09/16/equifax-legal/?iid=sr-link3> (last accessed October 24, 2017).

²⁸ <https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318> (last accessed October 23, 2017).

Committee, the former CEO of Equifax tied this colossal failure to an “individual” in its technology department who failed to implement the software fixes needed.²⁹ Apparently this individual “did not ensure communication got to the right person to manually patch the application.”³⁰ This error was then also missed by the scanning software Equifax employed to detect such vulnerabilities.³¹

92. That one person’s failure could result in a breach of this magnitude and that other fail safes were not in place to avoid such an error demonstrates a staggering level of incompetence and lack of reasonable precautions throughout Equifax.

93. Hackers piggybacked on the March intrusion by entering a computer command that gave them the username of the computer account to which they had gained access.³²

94. It is believed that this was part of a “months long reconnaissance mission” to test for further vulnerabilities.³³

95. In the interim, while the breach was still unknown to the public—but

²⁹ <https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html> (last accessed October 23, 2017).

³⁰ *Id.*

³¹ *Id.*

³² <https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617> (last accessed October 23, 2017).

³³ *Id.*

one day before and then the same day outside counsel was formally retained—Equifax’s Chief Legal Officer personally approved stock sales requested by three senior executives, including chief financial officer, John Gamble; President of U.S. information solutions, Joseph Loughran; and president of workforce solutions, Rodolfo Ploder; worth almost \$1.8 million in total. The shares were apparently not listed as part of a 10b5-1 scheduled trading plan.³⁴

96. Equifax did not contact any of the state Attorneys General about the breach beforehand to alert them, as is required by several state laws.³⁵

97. Even more egregious, in the months before the Data Breach, Equifax had lobbied for less regulation in the realm of data security, spending at least \$500,000 in the first half of 2017—*while the Equifax Data Breach was occurring*.³⁶ Top among the issues it lobbied was limiting the legal liability of credit reporting companies like itself.³⁷

³⁴ <http://www.law.com/sites/almstaff/2017/10/03/equifax-retained-law-firm-a-month-before-notifying-public-of-data-breach/> (last accessed October 23, 2017); <https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe> (last accessed October 23, 2017).

³⁵ <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?rref=collection%2Fbyline%2Fron-lieber> (last accessed October 23, 2017).

³⁶ https://www.wsj.com/articles/equifax-lobbied-for-easier-regulation-before-data-breach-1505169330?shareToken=st2add8019719c47d29a833f397f01a258&reflink=article_email_share (last accessed October 23, 2017).

³⁷ *Id.*

D. Equifax Fumbles When It Finally Alerts Customers

98. Despite enlisting the aid of outside counsel with a data security team on July 31, 2017 and notifying the FBI on August 2, 2017, Equifax waited more than a month to notify the public of the massive breach.³⁸

99. Equifax did not even notify the chairman of its board of directors until August 22, 2017 and waited two more days to inform the full board. The company then waited two additional weeks to tell the public.³⁹

100. Equifax announced the breach in a press release published on its website on September 7, 2017.⁴⁰ The release did not mention when the breach had occurred. Equifax conceded that for 143,000,000 consumers, “[t]he information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver’s license numbers.”

101. The number of consumers impacted by the breach has already risen substantially and is expected to continue to rise. The latest release provides that 145,500,000 consumers may have been impacted.⁴¹

³⁸ <http://www.law.com/sites/almstaff/2017/10/03/equifax-retained-law-firm-a-month-before-notifying-public-of-data-breach/> (last accessed October 23, 2017).

³⁹ *Id.*

⁴⁰ <https://www.equifaxsecurity2017.com/> (last accessed October 23, 2017).

⁴¹ <http://www.businessinsider.com/equifax-hack-millions-more-affected-2017-10> (last accessed October 23, 2017).

102. Furthermore, the hackers gained access to approximately 209,000 customers' credit card numbers, and had gained access to financial dispute documents containing personal identifying information for approximately 182,000 U.S. customers.⁴²

103. Post-breach, Equifax's website contained a link where consumers could provide their last name and the last six digits of their Social Security number to "[s]ee if [their] personal information was potentially impacted."⁴³ This link was circulated by countless online media companies, blogs, and social networks.

104. However, after completing this process many people simply received a notice to enroll in "TrustedId Premier," an Equifax credit monitoring service. Contrary to the solicitation by Equifax, the application did not indicate whether one's information had been potentially impacted.

105. Moreover, it was not clear from the website whether the terms of service applied. These terms included an arbitration clause and class waiver. After tech publications commented on this, Equifax spent the next several days trying to fix matters.

⁴² Equifax has not yet sent a letter or email to specific customers that it suspects may have had their personal identification information exposed to thieves. So far, the website is all that has been provided.

⁴³ <https://www.equifaxsecurity2017.com/> (last accessed November 7, 2017).

106. The site was panned as not only not helpful, but a “stalling tactic” and a “sham”:

WEB SITE WOES

As noted in yesterday’s breaking story on this breach, the Web site that Equifax advertised as the place where concerned Americans could go to find out whether they were impacted by this breach — equifaxsecurity2017.com — is completely broken at best, and little more than a stalling tactic or sham at worst.

In the early hours after the breach announcement, the site was being flagged by various browsers as a phishing threat. In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones. Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring service we were eligible for was not available and to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a reader’s comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.⁴⁴

107. Equifax’s (now former)⁴⁵ Chairman and Chief Executive Officer, Richard F. Smith, gave the following statement:

⁴⁴ <https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/> (last accessed October 23, 2017).

⁴⁵ Smith “retired” in the aftermath of the breach. <https://finance.yahoo.com/news/equifax-shares-halted-news-pending-124726108.html> (last accessed October 23, 2017).

This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes. We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations.⁴⁶

108. But Equifax was wholly unprepared to handle the traffic its website and phone lines would receive after announcing the breach of more than 143,000,000 people's personal financial information. Equifax's website and phone lines crashed repeatedly, leaving panicked consumers unable to determine whether their information was compromised. The website was similarly overwhelmed, frequently generating system error messages.⁴⁷

109. Equifax's former CEO admitted that Equifax was "disappointed" with the rollout of its website and call centers, and that it "struggled with the initial effort" to assist consumers after the breach.⁴⁸

110. Equifax's interim CEO, Paulino de Rego Barros Jr., has similarly acknowledged that "[a]nswers to key consumer questions were too often delayed,

⁴⁶ <https://www.cyberianit.com/2017/09/09/equifax-gets-breached-almost-150-million-people-could-be-affected/> (last accessed October 23, 2017).

⁴⁷ *Id.*

⁴⁸ <http://www.latimes.com/business/la-fi-equifax-data-breach-20171002-story.html> (last accessed October 23, 2017).

incomplete or both.”⁴⁹

111. Additionally, those consumers who did manage to get through to check whether they were affected were left confused when an apparent bug in the website coding gave consumers different results as to whether their information was compromised based on what browser they used. This lack of preparation for such an immensely foreseeable demand is inexplicable, and inexcusable, for an organization that holds itself out as an elite information technology company.

112. Additionally, the website Equifax set up to help consumers find out whether they were impacted by the breach was found to be vulnerable to hackers.⁵⁰

113. Equifax’s Twitter account also repeatedly tweeted a fake website called www.securityequifax2017.com instead of linking its actual website.⁵¹

114. Equifax’s Argentinian operations also continued to use “admin” as both a login and a password for an online employee tool a week after the Equifax Data Breach.⁵²

115. The breach led to scammers seeking to take advantage of consumers

⁴⁹ <https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html> (last accessed October 23, 2017).

⁵⁰ <http://fortune.com/2017/09/16/equifax-legal/?iid=sr-link3> (last accessed October 23, 2017).

⁵¹ <http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site> (last accessed October 23, 2017).

⁵² <http://www.bbc.com/news/technology-41257576> (last accessed October 24, 2017).

by sending email phishing scams trying to have already concerned consumers provide important information to other thieves.⁵³

116. Scammers were also able to successfully manipulate code on Equifax's website to prompt consumers to download a fraudulent update to Adobe Flash that installs adware, further exposing consumers' information.⁵⁴

117. Equifax has also attempted to *capitalize* on the Data Breach by pushing its own data-protection services.⁵⁵

118. Equifax persisted for days in charging many people for the privilege of freezing their credit files. Such a freeze is helpful because a new creditor cannot obtain a credit report on a person who has one and thus cannot loan money to a criminal impersonating that person. Equifax eventually relented due to public pressure, but those who were induced to pay for credit freezes as a result of Equifax's own actions and inactions suffered monetary damages.⁵⁶

119. Equifax's call center woes continue, with numerous reports that phone

⁵³ http://nypost.com/2017/09/24/this-equifax-e-mail-is-likely-a-scam/?utm_campaign=iosapp&utm_source=mail_app (last accessed October 23, 2017).

⁵⁴ https://www.washingtonpost.com/news/the-switch/wp/2017/10/12/equifax-says-its-looking-into-another-possible-hack/?utm_term=.da1498e543d9 (last accessed October 23, 2017).

⁵⁵ <http://www.npr.org/2017/09/14/550949718/after-equifax-data-breach-consumers-are-largely-on-their-own> (last accessed October 23, 2017).

⁵⁶ https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html?rref=collection%2Fbyline%2Fron-lieber&action=click&contentCollection=undefined®ion=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=collection (last accessed October 23, 2017).

representatives did not know how to answer questions regarding credit freezes and provided an alternate number to call that is actually a “triple-X hardcore service.”⁵⁷ Equifax has acknowledged “issues with our call centers” and says it is “working hard to provide additional training to [its] agents.”⁵⁸

120. Wait times continue to be high and website and phone issues persist.⁵⁹

E. Equifax Starts Laying Blame Elsewhere

121. The initial release did not identify the vulnerability that was exploited by hackers.

122. On September 13, 2017, Equifax posted the following:

1) Updated information on U.S. website application vulnerability. Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. **The vulnerability was Apache Struts CVE-2017-5638.** We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.

123. Apache did not accept the blame, and responded that the breach, “was due to [Equifax’s] failure to install the security updates provided in a timely

⁵⁷ <https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html> (last accessed October 23, 2017).

⁵⁸ *Id.*

⁵⁹ *Id.*

manner.”⁶⁰

124. On September 15, 2017, Equifax updated this site, and acknowledged Apache’s prior alert:

Questions Regarding Apache Struts

- The attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.
- Based on the company’s investigation, Equifax believes the unauthorized accesses to certain files containing personal information occurred from May 13 through July 30, 2017. The particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017.
- **Equifax’s Security organization was aware of this vulnerability at that time, and took efforts to identify and to patch any vulnerable systems in the company’s IT infrastructure.**
 - While Equifax fully understands the intense focus on patching efforts, the company’s review of the facts is still ongoing. The company will release additional information when available.⁶¹

⁶⁰ *Id.*

⁶¹ <https://www.equifaxsecurity2017.com/> (emphasis added) (last accessed October 23, 2017).

125. In fact, the list of Equifax's steps after announcement of the breach itemize the numerous things it had to fix, correct, and clarify, demonstrating its rank incompetence in handling its neglect:

- Since the announcement, Equifax has taken additional actions including:
 - **Providing a more prominent and clear** link from the main www.equifax.com website to the cybersecurity incident website www.equifaxsecurity2017.com, so that consumers can quickly and easily find the information they need.
 - **Tripling the call center team** and continuing to add agents, despite facing some difficulty due to Hurricane Irma.
 - **Resolving issues** with the impact look-up tool.
 - **Addressing confusion concerning the arbitration and class-action waiver clauses included in the Terms of Use applicable to the product:**
 - The company never intended for these clauses to apply to this cybersecurity incident.
 - Because of consumer concern, the company clarified that those clauses do not apply to this cybersecurity incident or to the complimentary TrustedID Premier offering.
 - **The company clarified that the clauses will not apply to consumers** who signed up before the language was removed.
 - **Clarifying that no credit card information is required to sign up for the product and that consumers will not be automatically enrolled or charged after the conclusion of the complimentary year.**
 - **Making changes to address consumer concerns regarding security freezes:**

- **The company clarified** that consumers placing a security freeze will be provided a randomly generated PIN.
- **The company continues to work on technical difficulties** related to the high volume of security freeze requests.
- **Consumers who paid for a security freeze starting at 5pm EST on September 7, 2017 will receive a refund.**
- The company agreed to waive fees for removing and placing security freezes through November 21, 2017.⁶²

126. Equifax's chief security officer was Susan Mauldin. Ms. Mauldin has a bachelor's degree and a master of fine arts degree in music composition. After the breach, Equifax started scrubbing its website of information about Ms. Mauldin, who retired shortly after the breach.⁶³

127. Since Ms. Mauldin's departure, Equifax's CEO and Chief Information Officer have also left.⁶⁴

128. Equifax has also reportedly pointed fingers at its security consulting partner, Mandiant, claiming that, in the days after the breach, it "sent rookies to

⁶² <https://www.equifaxsecurity2017.com/> (emphasis added) (last accessed October 23, 2017).

⁶³ <http://www.marketwatch.com/amp/story/guid/766FA70C-9A38-11E7-B604-EDFD35AE15F2> (last accessed October 23, 2017).

⁶⁴ <https://www.nbcnews.com/business/consumer/equifax-executives-step-down-scrutiny-intensifies-credit-bureaus-n801706> (last accessed October 23, 2017).

look into the vulnerabilities of its systems[.]”⁶⁵

F. Equifax Attempts to Leverage Its Negligence to Benefit Financially from the Harm It Caused

129. In a twist that will leave Equifax with yet more questions to answer, Equifax purchased an identification protection service called ID Watchdog on August 10, two weeks after Equifax discovered the breach but over a month before publicly disclosing it.⁶⁶

130. ID Watchdog, which Equifax purchased for \$62 million, monitors consumer credit and provides identity theft notifications.⁶⁷

131. There will be an increased need and market for such services in the wake of the Equifax Data Breach, and Equifax appears to have positioned itself to profit from the misfortune it created for consumers.

132. Equifax similarly stands to benefit from the 100,000 new customers LifeLock signed up the week after the breach at \$29.95 per month (as well as those who continue to sign up for LifeLock) since it receives a sizable cut of these

⁶⁵ <https://finance.yahoo.com/news/equifax-breach-shows-signs-possible-223100521.html> (last accessed October 23 2017).

⁶⁶ https://www.pymnts.com/news/security-and-risk/2017/equifax-bought-an-identity-protection-service-just-before-disclosing-the-breach/?utm_source=Push+Notifications&utm_medium=Push+Notifications&utm_campaign=Push+Notifications (last accessed October 23, 2017).

⁶⁷ *Id.*

customers' fees.⁶⁸

133. Equifax's former CEO noted as recently as August 17, 2017 that "[f]raud is a huge opportunity for us—it's a massive, growing business for us."⁶⁹

134. On August 17, 2017, according to his own testimony before the United States House of Representatives, Equifax's former CEO was already aware "that it appeared likely that consumer PII [*i.e.*, Personally Identifiable Information] had been stolen."⁷⁰

135. As Senator Elizabeth Warren said during a recent hearing before the Senate Banking Committee, "Equifax is making money—millions of dollars—off its own screw-up." Senator Warren also pointed out that "[b]ecause of this breach, consumers will spend the rest of their lives worrying about identity theft. But Equifax will be just fine—heck, it could actually come out ahead."⁷¹

G. The Lasting Impact of Equifax's Negligence is Just Starting to be Felt

136. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2008:

⁶⁸ <https://boingboing.net/2017/10/05/failing-up-and-up.html> (last accessed October 23, 2017).

⁶⁹ <http://time.com/money/4969163/equifax-hearing-elizabeth-warren-richard-smith/> (last accessed October 23, 2017).

⁷⁰ <http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf> (last accessed October 23, 2017).

⁷¹ *Id.*

In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.⁷²

137. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁷³

⁷² The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, at p. 11 (April 2007), available at <http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf>.

⁷³ U.S. Government Accountability Office, *Report to Congressional Requesters*, at p. 29 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf>.

138. The unauthorized disclosure of Social Security Numbers can be particularly damaging, because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, *inter alia*, that he or she continues to be disadvantaged by the misuse. Thus, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other personal information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you will not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.⁷⁴

139. Personal and financial information such as that stolen in the Equifax

⁷⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, Social Security Administration Publication No. 05-10064, at p.7-8 (Aug. 2009), available at <http://www.ssa.gov/pubs/10064.html>.

Data Breach is highly coveted by, and a frequent target of, hackers. For example:

- Thieves use the credit card information to create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards;
- Thieves reproduce stolen debit cards and use them to withdraw cash from ATMs;
- Thieves can use the victim's personal information to commit immigration fraud, obtain a driver's license or identification card in the victim's name but with another's picture, use the victim's information to obtain government benefits, or file a fraudulent tax return using the victim's information to obtain a fraudulent refund; or get medical services using consumers' stolen information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

140. Equifax has consciously worked to assemble a massive stash of private employment and salary history information, information that is now exposed and susceptible to use by bad actors.⁷⁵

141. Specifically, because home buyers and mortgage applicants tend to have significant information on file with credit bureaus, they are especially at risk for identity theft after the Equifax Data Breach. Identity theft during an important purchase like buying a home is particularly devastating and creates significant

⁷⁵ <https://krebsonsecurity.com/2017/10/equifax-breach-fallout-your-salary-history/> (last accessed October 23, 2017).

legal and financial issues.⁷⁶

142. Lenders are also concerned that consumers will take out fewer loans and credit cards if more people are locking or freezing their credit reports, hurting that industry.⁷⁷

143. A cyber black market exists in which criminals openly post and sell stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites.

144. There are reports that information from the Equifax Data Breach is already for sale on one such black market, known as the Dark Web.⁷⁸

145. Avivah Litam, a fraud analyst at leading information technology consulting and research firm, Gartner, Inc., describing the Equifax breach, said, “[o]n a scale of 1-to 10 in terms of risk to consumers, this a 10.”⁷⁹

146. Senator Mark Warner of Virginia stated, “It is no exaggeration to suggest that a breach such as this — exposing highly sensitive personal and

⁷⁶ https://www.washingtonpost.com/realestate/theft-of-data-could-lead-to-years-of-grief-for-home-buyers-and-mortgage-applicants/2017/09/12/ed0f66fc-971a-11e7-82e4-f1076f6d6152_story.html (last accessed October 23, 2017).

⁷⁷ <https://www.pymnts.com/news/security-and-risk/2017/equifax-credit-freezes-worry-lenders-after-data-breach/> (last accessed October 23, 2017).

⁷⁸ <http://fortune.com/2017/09/16/equifax-legal/?iid=sr-link3> (last accessed October 24, 2017).

⁷⁹ <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=3> (last accessed October 23, 2017).

financial information central for identity management and access to credit — represents a real threat to the economic security of Americans.”⁸⁰

147. Massachusetts Attorney General Maura Healey called the Equifax Data Breach “the most brazen failure to protect consumer data we have ever seen.”⁸¹

148. In written testimony for his hearing with the House Energy and Commerce Committee, former Equifax CEO Richard Smith stated, “Equifax was entrusted with Americans’ private data and we let them down,” acknowledged the “human error” involved, and said that “[t]he company failed to prevent sensitive information from falling into the hands of wrongdoers.”⁸²

149. The foregoing is yet more concerning when one considers that there does not appear to be a way to “opt out” of Equifax’s data collection, or request that it delete consumers’ files, and stop making money off of consumers’ most private data.⁸³

⁸⁰ <http://www.chicagotribune.com/business/national/ct-equifax-data-breach-20170907-story.html> (last accessed October 23, 2017).

⁸¹ <http://www.npr.org/2017/09/14/550949718/after-equifax-data-breach-consumers-are-largely-on-their-own> (last accessed October 24, 2017).

⁸² <http://www.latimes.com/business/la-fi-equifax-data-breach-20171002-story.html> (last accessed October 23, 2017).

⁸³ <https://www.nytimes.com/2017/10/06/your-money/credit-scores/equifax-hack.html> (last accessed October 23, 2017).

150. During his testimony before the United States Senate, Equifax's former CEO conceded that he did not think that people should not be able to delete their data from Equifax's systems.⁸⁴

151. Equifax's action and failure to act when required has caused Plaintiffs and millions of others to suffer harm and/or face the significant risk of future harm, including but not limited to:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their personal and financial information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach—

⁸⁴ *Id.*

including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts—and the stress, nuisance, and annoyance of dealing with all issues resulting from the Equifax Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet card black market;

g. damages to and diminution in value of their personal and financial information entrusted, directly or indirectly, to Equifax with the mutual understanding that Equifax would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

h. continued risk to their financial and personal information, which remains in Equifax's possession and is subject to further

breaches so long as Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs.

V. CLASS ALLEGATIONS

152. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert that Equifax violated the FCRA, as well as common law claims for negligence, negligence *per se*, bailment, and unjust enrichment, as well as declaratory and injunctive relief, on behalf of themselves and the following nationwide class (“the Nationwide Class” or the “Class”):

NATIONWIDE CLASS

All residents of the United States whose Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017.

Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert statutory claims under state consumer protection statutes and state data breach statutes, on behalf of separate statewide subclasses for each of the 50 states and the District of Columbia (the “Subclass” or “Subclasses”), defined as follows:

STATEWIDE [NAME OF STATE] SUBCLASS:

All residents of the [name of state] whose Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017.

153. Excluded from the foregoing Nationwide Class and Subclasses are

Equifax, any entity in which Equifax has a controlling interest, and Equifax's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the nationwide class and subclasses is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

154. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiffs are informed and believe—based upon Equifax's press releases—that there are over 145 million Class members. Those individuals' names and addresses are available from Equifax's records, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice.

155. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

- a. Whether Equifax knew or should have known that its computer systems were vulnerable to attack;

- b. Whether Equifax failed to take adequate and reasonable measures to ensure its data systems were protected;
- c. Whether Equifax failed to take available steps to prevent and stop the breach from ever happening;
- d. Whether Equifax failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard consumers' financial and personal data;
- e. Whether Equifax failed to provide timely and adequate notice of the data breach;
- f. Whether Equifax owed a duty to Plaintiffs and the other Class and Subclass Members to protect their personal and financial information and to provide timely and accurate notice of the data breach to Plaintiffs and the other Class and Subclass Members;
- g. Whether Equifax breached its duties to protect the personal and financial information of Plaintiffs and the other Class and Subclass Members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiffs and the other Class and Subclass Members of the data breach;
- h. Whether Equifax's conduct, including its failure to act, resulted

in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of millions of consumers' personal and financial information;

i. Whether Equifax's conduct amounted to violations of the FCRA (15 USC §§ 1681, *et seq.*), state consumer protection acts, and state data breach acts;

j. Whether Equifax's conduct renders it liable for negligence, negligence *per se*, bailment, and unjust enrichment;

k. Whether, as a result of Equifax's conduct, Plaintiffs and the other Class and Subclass Members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

l. Whether, as a result of Equifax's conduct, Plaintiffs and the other Class and Subclass Members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

156. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the other Class members' claims because Plaintiffs and the

other Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

157. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate class representatives because their interests do not conflict with the interests of the other Class members who they seek to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

158. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Equifax. Such individual actions would create a risk of adjudications which would be dispositive of the interests of other Class members and impair their interests. Equifax has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

159. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient

adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Equifax, so it would be impracticable for Class members to individually seek redress for Equifax's wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED ON BEHALF OF THE NATIONWIDE CLASS

FIRST CAUSE OF ACTION

FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681, *ET SEQ.* (ASSERTED BY THE NATIONWIDE CLASS)

160. Plaintiffs, individually and on behalf of the other Nationwide Class members, repeat and reallege Paragraphs 1-160, as if fully alleged herein.

161. Plaintiffs and each of the other Class members are "consumers," as

defined in 15 U.S.C. § 1681a(c).

162. Equifax is a “consumer reporting agency” and a “consumer reporting agency that compiles and maintains files on consumers on a nationwide basis” as defined in 15 U.S.C. §§ 1681a(f) and (p), respectively.

163. Equifax compiled and maintained a “consumer report” on Plaintiffs and the other Class members, as defined in 15 U.S.C. § 1681a(d): a “written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under section 1681b of this title.”

164. Under the Fair Credit Reporting Act (“FCRA”), Equifax had an obligation to protect from disclosure Plaintiffs’ and the other Class members’ consumer reports under the circumstances alleged herein. Section 1681b prohibits a consumer reporting agency from disclosing a consumer report except as permitted under the statute.

165. Section 1681e of the FCRA requires every consumer reporting agency

to maintain reasonable procedures designed to avoid violations of the FCRA and to limit the furnishing of consumer reports to the purposes permitted under the statute.

166. As a direct and proximate result of Equifax's actions and failures to act described herein, including, without limitation, its failure to take adequate and reasonable measures to ensure its data systems were protected, and failure to take appropriate steps to prevent and stop the data breach from ever happening, Equifax allowed unauthorized criminal computer hackers to obtain consumer reports of Plaintiffs and the other Class members.

167. Equifax's disclosure of consumer reports under these circumstances was not permitted by, and thus in violation of, Sections 1681b and e of the FCRA.

168. As a direct and proximate result of Equifax's actions and failures to act described herein, including, without limitation, its failure to take adequate and reasonable measures to ensure its data systems were protected, and failure to take appropriate steps to prevent and stop the data breach from ever happening, Equifax caused Plaintiffs and the other Class members to suffer harm and/or face the significant risk of harm in the future, including, among other things, the harm and threat of harm described above.

169. Under Section 1681o of the FCRA, Equifax is liable to Plaintiffs and

the other Class members for negligently failing to comply with the requirements not to disclose consumer reports, and to take measures designed to avoid the unauthorized disclosure of consumer reports. Equifax therefore is liable to Plaintiffs and the other Class members for any actual damages they sustain as a result of Equifax's failure, as well as costs and reasonable attorneys' fees, in amounts to be proven at trial.

170. In addition, Equifax's failure to comply with the foregoing requirements was willful because, upon information and belief, Equifax knew or should have known, but recklessly disregarded, that its cybersecurity measures were not adequate and reasonable to protect consumers' sensitive financial and personal data from security breaches.

171. Therefore, Equifax is liable to Plaintiffs and the other Class members in an amount equal to actual damages, or damages of not less than \$100 and not more than \$1,000 for each Plaintiff and other Class member, as well as punitive damages as the Court may allow.

SECOND CAUSE OF ACTION

NEGLIGENCE

(Asserted by Plaintiffs, individually, and on behalf of the Nationwide class, and, in the alternative, Statewide Subclasses)

172. Plaintiffs, individually and on behalf of the other Nationwide Class

members, repeat and reallege Paragraphs 1-160, as if fully alleged herein.

173. Equifax owed a duty to Plaintiffs and the other Nationwide Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's security systems to ensure that Plaintiffs' and the other Nationwide Class members' personal and financial information in Equifax's possession was adequately secured and protected. Equifax further owed a duty to Plaintiffs and the other Nationwide Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

174. Equifax owed a duty to Plaintiffs and the other Nationwide Class members to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiffs and the other Nationwide Class members about whom Equifax collected, maintained, and used such information.

175. Equifax owed a duty of care to Plaintiffs and the other Nationwide Class members because they were foreseeable and probable victims of any inadequate security practices. Equifax solicited, gathered, and stored the personal and financial data provided by Plaintiffs and the other Nationwide Class members to facilitate its provision of credit score and other financial information to customers. Equifax knew it inadequately safeguarded such information on its computer systems and that hackers routinely attempted to access this valuable data without authorization.

176. Equifax's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair...practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Equifax. Various FTC publications and data security breach orders further form the basis of Equifax's. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

177. Equifax knew that a breach of its systems would cause damages to Plaintiffs and the other Nationwide Class members and Equifax had a duty to adequately protect such sensitive financial and personal information.

178. Equifax owed a duty to timely and accurately disclose to Plaintiffs and the other Nationwide Class members that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiffs and the other Nationwide Class members could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by Equifax's misconduct.

179. Plaintiffs and the other Nationwide Class members entrusted, directly and indirectly, Equifax with their personal and financial information, on the premise and with the understanding that Equifax would safeguard their information, and Equifax was in a position to protect against the harm suffered by Plaintiffs and the other Nationwide Class members as a result of the Equifax data breach.

180. Equifax knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and the

other Nationwide Class members and of the critical importance of providing adequate security of that information.

181. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and the other Nationwide Class members. Equifax's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the data breach as set forth herein. Equifax's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the personal and financial information of Plaintiffs and the other Nationwide Class members.

182. Equifax breached the duties it owed to Plaintiffs and the other Nationwide Class members by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal and financial information of Plaintiffs and the other Nationwide Class members.

183. Equifax breached the duties it owed to Plaintiffs and the other Nationwide Class members by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

184. Equifax breached the duties it owed to Plaintiffs and the other Nationwide Class members by failing to properly maintain their sensitive personal and financial information. Given the risk involved and the amount of data at issue,

Equifax's breach of its duties was entirely unreasonable.

185. Equifax breached its duties to timely and accurately disclose that Plaintiffs' and the other Nationwide Class members' personal and financial information in Equifax's possession had been or was reasonably believed to have been, stolen or compromised.

186. Equifax's failure to comply with its legal obligations and with industry standards and regulations, and the delay between the date of intrusion and the date Equifax disclosed the data breach, further evidence Equifax's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Nationwide Class members' personal and financial information in Equifax's possession.

187. Equifax knew that Plaintiffs and the other Nationwide Class members were foreseeable victims of a data breach of its systems because of laws and statutes that require Equifax to reasonably safeguard sensitive payment information, as detailed herein.

188. But for Equifax's wrongful and negligent breach of its duties owed to Plaintiffs and the other Nationwide Class members, their personal and financial information would not have been compromised.

189. The injury and harm suffered by Plaintiffs and members of the

Nationwide Class as set forth above was the reasonably foreseeable result of Equifax's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Nationwide Class members' personal and financial information within Equifax's possession. Equifax knew or should have known that its systems and technologies for processing, securing, safeguarding and deleting Plaintiffs' and the other Nationwide Class members' personal and financial information were inadequate and vulnerable to being breached by hackers.

190. Plaintiffs and the other Nationwide Class members suffered injuries and losses described herein as a direct and proximate result of Equifax's conduct resulting in the data breach, including Equifax's lack of adequate reasonable and industry standard security measures. Had Equifax implemented such adequate and reasonable security measures, Plaintiffs and the other Nationwide Class members would not have suffered the injuries alleged, as the Equifax data breach would likely have not occurred.

191. As a direct and proximate result of Equifax's negligent conduct, Plaintiffs and the other Nationwide Class members have suffered injury and the significant risk of harm in the future, and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION

NEGLIGENCE *PER SE*

(Asserted by Plaintiffs, individually, and on behalf of the Nationwide class, and, in the alternative, Statewide Subclasses)

192. Plaintiffs, individually and on behalf of the other Nationwide Class members, repeat and reallege Paragraphs 1-160, as if fully alleged herein.

193. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair...practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by companies such as Equifax of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Equifax’s duty.

194. Equifax violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Equifax’s conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach at one of the three major credit bureaus.

195. Equifax’s violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

196. The Nationwide Class and the alternative state specific classes are

within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Plaintiffs and absent class members are consumers.

197. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs, the Nationwide Class and the alternative state specific classes.

198. As a direct and proximate result of Equifax's negligence *per se*, the Plaintiffs, the Nationwide Class and the alternative state specific classes have suffered and continue to suffer injury, including but not limited to:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their personal and financial information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being

limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax data breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet card black market;

g. damages to and diminution in value of their personal and

financial information entrusted to Equifax with the mutual understanding that Equifax would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

h. continued risk to their financial and personal information, which remains in Equifax's possession and is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs.

FOURTH CAUSE OF ACTION

BAILMENT

(Asserted by Plaintiffs, individually, and on behalf of the Nationwide class, and, in the alternative, Statewide Subclasses)

199. Plaintiffs, individually and on behalf of the other Nationwide Class members, repeat and reallege Paragraphs 1- 160, as if fully alleged herein.

200. Plaintiffs and the other Class members provided, or authorized disclosure of, their personal and financial information to Equifax for the exclusive purpose of Equifax preparing consumer reports, credit monitoring and identity theft protection, and similar services and legitimate business uses.

201. In allowing their personal and financial information to be made available to Equifax, Plaintiffs and the other Class members intended and

understood that Equifax would adequately safeguard their personal and financial information.

202. Equifax accepted possession of Plaintiffs' and the other Class members' personal and financial information for the purpose of making available to Plaintiffs and the other Class members Equifax's services for their benefit.

203. By accepting possession of Plaintiffs' and the other Class members' personal and financial information, Equifax understood that Plaintiffs and the other Class members expected Equifax to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Equifax owed a duty to Plaintiffs and the other Class members to exercise reasonable care, diligence, and prudence in protecting their personal and financial information.

204. Equifax breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and the other Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and the other Class members' personal and financial information.

205. Equifax further breached its duty to safeguard Plaintiffs' and the other Class members' personal and financial information by failing to timely and

accurately notify them that their information had been compromised as a result of the Equifax Data Breach.

206. As a direct and proximate result of Equifax's breach of its duty, Plaintiffs and the other Class members suffered consequential damages that were reasonably foreseeable to Equifax, including but not limited to the damages set forth above.

207. As a direct and proximate result of Equifax's breach of its duty, the personal and financial information of Plaintiffs and the other Class members entrusted, directly or indirectly, to Equifax during the bailment (or deposit) was damaged and its value diminished.

FIFTH CAUSE OF ACTION

UNJUST ENRICHMENT

(Asserted by Plaintiffs, individually, and on behalf of the Nationwide class, and, in the alternative, Statewide Subclasses)

208. Plaintiffs, individually and on behalf of the other Nationwide Class members, repeat and reallege Paragraphs 1-160, as if fully alleged herein.

209. Plaintiffs, Class members, and others conferred benefits upon Equifax in the form of sensitive information of Plaintiffs and the other Class members, monies paid by others to access that sensitive information, and monies paid by Plaintiffs and Class members who purchased services from Equifax.

210. Equifax appreciates or has knowledge of the benefits conferred directly upon it by Plaintiffs, Class members, and others.

211. As a result of Equifax's wrongful conduct as alleged herein, Equifax has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the other Class members.

212. Equifax's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and the other Class members' sensitive personal and financial information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

213. Under the common law doctrine of unjust enrichment, it is inequitable for Equifax to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs, Class members, and others in an unfair and unconscionable manner. Equifax's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

214. Plaintiffs, Class members, and others did not confer these benefits officiously or gratuitously, and it would be inequitable and unjust for Equifax to retain these wrongfully obtained profits.

215. Equifax is therefore liable to Plaintiffs and the other Class members

for restitution in the amount of the benefit conferred on Equifax, including specifically Equifax's wrongfully obtained profits.

**VII. STATE CONSUMER PROTECTION LAWS BROUGHT BY THE
STATEWIDE SUBCLASSES BELOW**

ALABAMA

SIXTH CAUSE OF ACTION

**ALABAMA DECEPTIVE TRADE PRACTICES ACT,
Ala. Code §§8-19-1, *et seq.*
(Asserted by the Alabama Subclass)**

216. Plaintiff Vanuel Harris ("Plaintiff," for purposes of this Count) individually and on behalf of the other Alabama Subclass members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

217. Plaintiff sent pre-suit notice pursuant to Ala. Code § 8-19-10(e) on October 10, 2017.

218. Equifax operating in Alabama engaged in deceptive acts and practices in the conduct of trade or commerce in violation of the Alabama Deceptive Trade Practices Act, which prohibits "(5) [r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have," "(7) [r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another," and "(27) [e]ngaging in any other unconscionable, false,

misleading, or deceptive act or practice in the conduct of trade or commerce,” Ala.

Code § 8-19-5, including but not limited to the following:

- a. Failing to enact adequate privacy and security procedures and practices to protect Alabama Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;
- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard the Alabama Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft;
- d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for the Alabama Subclass Members’ Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws

pertaining to the privacy and security of the Alabama Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA; and

f. Failing to maintain the privacy and security of the Alabama Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the foregoing paragraph, directly and proximately causing the Equifax Data Breach.

219. As a direct and proximate result of Equifax's unlawful practices, Alabama Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

220. The foregoing unlawful and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Alabama Subclass Members that they could not reasonably avoid, and this substantial injury outweighed any benefits to consumers or to competition.

221. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Alabama Subclass Members' Personal Information and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the abovenamed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Alabama Subclass members.

222. Pursuant to Ala. Code § 8-19-10, Plaintiffs and the Alabama Subclass seek monetary relief against Equifax measured as the greater of (a) actual damages in an amount to be determined at trial and (b) statutory damages in the amount of \$100 for each Plaintiff and each Alabama Subclass Member.

223. Plaintiffs and Alabama Subclass Members also seek an order enjoining Equifax's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1, et seq.

ALASKA

SEVENTH CAUSE OF ACTION

**ALASKA CONSUMER PROTECTION ACT,
AS §§ 45.50.471, et seq.
(Asserted by the Alaska Subclass)**

224. Plaintiff Michael Bishop ("Plaintiff," for purposes of this Count),

individually and on behalf of the other Alaska Subclass Members, repeats and realleges Paragraphs 1-160, as if fully alleged herein.

225. Equifax operating in Alaska is engaged in trade or commerce in the State of Alaska.

226. Equifax engaged in unfair acts and practices with the capacity or tendency to deceive (as defined in the Alaska Consumer Protection Act, AS §§ 45.50.471-A.S. 45.50.561) in violation of AS § 45.50.471, including but not limited to:

- a. Representing that its goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have in violation of AS § 45.50.471(4);
- b. Representing that its goods or services are of a particular standard, quality, or grade, when they are of another in violation of AS § 45.50.471(6);
- c. Advertising its goods or services with intent not to sell them as advertised in violation of AS § 45.50.471(8);
- d. Engaging in other conduct creating a likelihood of confusion or of misunderstanding and which misleads, deceives, or damages a buyer in connection with the sale or advertisements of its goods or

services in violation of AS § 45.50.471(11); and

e. Using or employing deception, fraud, false pretense, false promise, misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that others rely upon the concealment, suppression, or omission in connection with the sale or advertisement of its goods or services whether or not a person was in fact misled, deceived, or damaged in violation of AS § 45.50.471(12).

227. The above unfair and deceptive practices and acts by Equifax were unlawful, contrary to public policy, immoral, unethical, unscrupulous, and oppressive, and caused substantial injury to consumers in the Alaska Subclass.

228. Plaintiff and Alaska Subclass Members seek relief under AS §§ 45.50.471, *et seq.*, including, but not limited to, compensatory damages, punitive damages, injunctive relief, and/or attorneys' fees and costs.

ARIZONA

EIGHTH CAUSE OF ACTION

ARIZONA CONSUMER FRAUD ACT, A.R.S. §§ 44-1521, *et seq.* (Asserted by the Arizona Subclass)

229. Plaintiff Zacariah Hildenbrand ("Plaintiff," for purposes of this Count), individually and on behalf of the other Arizona Subclass Members, repeats

and alleges Paragraphs 1-160, as if fully alleged herein.

230. Equifax operating in Arizona engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of “merchandise” (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A), including but not limited to the following:

- a. Misrepresenting material facts to Arizona Subclass Members in connection with the sale of its products and services by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Arizona Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts to Arizona Subclass Members in connection with the sale of its products and services by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Arizona Subclass Members’ Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Arizona

Subclass Members' Personal Information, with the intent that others rely on the omission, suppression, and concealment;

d. Engaging in unfair acts and practices in connection with the sale of its products and services by failing to maintain the privacy and security of Arizona Subclass Members' Personal Information in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GBLA.

e. Engaging in unfair acts and practices in connection with the sale of its products and services by failing to disclose the Equifax Data Breach to Arizona Subclass Members in a timely and accurate manner, in violation of A.R.S. § 44-7501; and

f. Engaging in unfair acts and practices with respect to the sale of its products and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Arizona Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

231. The above unfair and deceptive practices and acts by Equifax were

immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Arizona Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

232. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Arizona Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Arizona Subclass.

233. As a direct and proximate result of Equifax's unlawful practices, Arizona Subclass Members suffered injury and/or damages.

234. Plaintiff and Arizona Subclass Members seek relief under A.R.S. §§ 4421, *et seq.*, including, but not limited to, compensatory damages, punitive damages, injunctive relief, and/or attorneys' fees and costs.

ARKANSAS

NINTH CAUSE OF ACTION

**ARKANSAS DECEPTIVE TRADE PRACTICES ACT,
A.C.A. §§ 4-88-101, *et seq.*
(Asserted by the Arkansas Subclass)**

235. Plaintiff Jerry Allen (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Arkansas Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

236. The Arkansas Deceptive Trade Practices Act (“ADTPA”), A.C.A. §§ 4-88-101, *et seq.*, prohibits deceptive, unfair, and unconscionable trade practices.

237. The ADTPA is a remedial statute which is to be liberally construed in favor of consumers.

238. Equifax is a “person” as defined by A.C.A. § 4-88-102(5).

239. Equifax’s products and services are “goods” and “services” as defined by A.C.A. §§ 4-88-102(4) and (7).

240. Equifax operating in Arkansas engaged in consumer transactions with Plaintiff and Arkansas Subclass Members that were intended to result in, and did result in, the sale of its products and services to Plaintiff and Arkansas Subclass Members.

241. Equifax’s conduct as described herein constitutes deceptive, unfair,

and unconscionable trade practices that are substantially injurious to consumers, as defined by A.C.A. §§ 4-88-107 and 4-88-108, with regard to its products and services, including but not limited to:

- a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;
- b. Advertising goods or services with the intent not to sell them as advertised;
- c. Other acts demonstrating an intent not to sell the advertised product or services;
- d. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade;
- e. Acting, using or employing deception, fraud, or false pretense; and
- f. Concealing, suppressing, or omitting material facts with intent that others rely upon the concealment, suppression, or omission.

242. Equifax knew, or should have known, that its representations and material omissions were unsubstantiated, false, unfair, deceptive and/or

unconscionable and otherwise have no reasonable basis in fact.

243. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Arkansas Subclass Members have been damaged and are entitled to relief, including but not limited to compensatory damages, civil penalties, equitable relief, injunctive relief to enjoin Equifax on terms that the Court deems reasonable, and attorneys' fees.

CALIFORNIA

TENTH CAUSE OF ACTION

**CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(Asserted by the California Subclass)**

244. Plaintiff Miche' Sharpe ("Plaintiff," for purposes of this Count), individually and on behalf of the other California Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

245. Equifax operating in California has violated Cal. Bus. & Prof. Code §§ 17200 *et seq.* by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200 with respect to the products and services provided to the Plaintiff and the California Subclass, including but not limited to the following:

a. Engaging in deceptive acts and practices with regard to the products and services provided to the California Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard California Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft; representing and advertising that it did and would comply with the requirements of federal and state laws pertaining to the privacy and security of California Subclass Members' Personal Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for California Subclass Members' Personal Information;

b. Engaging in unfair acts and practices with respect to the products and services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass Members' Personal Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Subclass Members' Personal Information in an unsecure electronic

environment. These unfair acts and practices were immoral unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Subclass Members. Equifax's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted, directly or indirectly, with personal data utilize appropriate security measures, as reflected by laws like the FCRA, the GLBA, and California's data breach statute (Cal. Civ. Code § 1798.81.5). The harm these practices caused to Plaintiff and California Subclass Members outweighed their utility, if any;

c. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to California Subclass Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Subclass Members. The harm these practices caused to Plaintiff and California Subclass Members outweighed their utility, if any;

- d. Engaged in unfair acts and practices with respect to the provision of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect California Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Subclass Members. The harm these practices caused to Plaintiff and the California Subclass Members outweighed their utility, if any; and
- e. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

246. As a direct and proximate result of Equifax's unfair and unlawful practices and acts, Plaintiff and California Subclass Members were injured and lost money or property, including but not limited to the premiums and/or price received by Equifax for its goods and services, the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and additional losses described above.

247. Equifax knew or should have known that its computer systems and

data security practices were inadequate to safeguard California Subclass Members' Personal Information and that the risk of a data breach or theft was high. Equifax's actions in engaging in the abovenamed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

248. Plaintiff and California Subclass Members seek relief under Cal. Bus. & Prof. Code §§ 17200 *et seq.*, including, but not limited to, restitution to Plaintiff and California Subclass Members of money or property that Equifax may have acquired by means of its deceptive, unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Equifax because of its unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civil Pro §1021.5), and injunctive or other equitable relief.

ELEVENTH CAUSE OF ACTION

CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq.* (Asserted by the California Subclass)

249. Plaintiff Miche' Sharpe ("Plaintiff," for purposes of this Count), individually and on behalf of the other California Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

250. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*

(“CLRA”) is a comprehensive statutory scheme that prohibits deceptive practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

251. Equifax is a “person” as defined by Civil Code § 1761(c).

252. Plaintiff and California Subclass Members are “consumers” within the meaning of Civil Code § 1761(d).

253. Equifax sells “goods” as defined by Civil Code § 1761(a).

254. Equifax provides “services” as defined by Civil Code § 1761(b).

255. Equifax’s sales of goods and services to Plaintiff and California Subclass Members constitute “transactions” which were “intended to result or which result[ed]” in the sale of goods and/or services to consumers within the meaning of Civil Code § 1761(e).

256. Plaintiff has standing to pursue this claim as she has suffered injury in fact and has lost money as a result of Equifax’s actions as set forth herein. Specifically, Plaintiff’s Personal Information has been compromised and she is imminently threatened with financial and identity theft, and, in fact, many have already suffered actual fraud.

257. Equifax operating in California has violated the CLRA by engaging in unlawful, unfair and deceptive practices as defined in Civil Code § 1770 with

respect to the products and services provided to Plaintiff and the California

Subclass, including but not limited to the following:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or trade when they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

258. Plaintiff, individually and on behalf of the California Subclass, seeks an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COLORADO

TWELFTH CAUSE OF ACTION

COLORADO CONSUMER PROTECTION ACT, Colo. Rev. Stat. §§ 6-1-101, *et seq.* (Asserted by the Colorado Subclass)

259. Plaintiff Gerald Muhammad ("Plaintiff," for purposes of this Count),

individually and on behalf of the other Colorado Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

260. Plaintiff and Colorado Subclass Members are actual or potential consumers of the products and services offered by Equifax.

261. Equifax operating in Colorado engaged in deceptive, unfair, and unlawful trade acts or practices in the course of its business, vocation or occupation, in violation of Colo. Rev. Stat. § 6-1-105, including but not limited to the following:

- a. Knowingly misrepresenting and fraudulently advertising material facts pertaining to its products and services to the Colorado Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Colorado Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, in violation of Colo. Rev. Stat. §§ 6-1-105(e), (g), (i), and (u);
- b. Knowingly misrepresenting material facts pertaining to its products and services to the Colorado Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security

of Colorado Subclass Members' Personal Information, in violation of Colo. Rev. Stat. §§ 6-1-105(e), (g), (i), and (u);

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Colorado Subclass Members' Personal Information (intending to induce others to enter into a transaction), in violation of Colo. Rev. Stat. §§ 6-1-105(e), (g), (i), and (u);

d. Engaging in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to maintain the privacy and security of Colorado Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GBLA;

e. Engaging in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to disclose the Equifax Data Breach to Colorado Subclass Members in a timely and accurate manner, contrary to the duties imposed by Colo.

Rev. Stat. § 6-1-716(2); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Colorado Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

262. Equifax engaged in the above unfair and deceptive acts or practices in the course of its business.

263. As a direct and proximate result of Equifax's deceptive trade practices, Colorado Subclass Members suffered injuries to legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

264. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Colorado Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

265. Equifax knew or should have known that its computer systems and

data security practices were inadequate to safeguard Colorado Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Colorado Subclass.

266. Plaintiff and Colorado Subclass Members seek relief under Colo. Rev. Stat. §§ 6-1-101, *et seq.*, including, but not limited to, compensatory damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

CONNECTICUT

THIRTEENTH CAUSE OF ACTION

CONNECTICUT UNFAIR TRADE PRACTICES ACT, C.G.S. §§ 42-110a *et seq.* (Asserted by the Connecticut Subclass)

267. Plaintiff Linda DeVore ("Plaintiff," for purposes of this Count), individually and on behalf of the other Connecticut Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

268. Equifax operating in Connecticut engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of C.G.S. § 42-110b, including but not limited to the following:

- a. Misrepresenting and fraudulent advertising material facts pertaining to its goods and services to the Connecticut Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Connecticut Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts pertaining to its goods and services to the Connecticut Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Connecticut Subclass Members' Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Connecticut Subclass Members' Personal Information;
- d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Connecticut Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair

acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, and the Connecticut data breach statute (C.G.S. § 42-471);

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Equifax Data Breach to Connecticut Subclass Members in a timely accurate manner, contrary to duties imposed by C.G.S. § 36a-701b; and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Connecticut Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

269. As a direct and proximate result of Equifax's deceptive trade practices, Connecticut Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

270. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Connecticut Subclass members that they could not

reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

271. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Connecticut Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

272. Plaintiff and Connecticut Subclass Members seek relief under C.G.S. §§ 42-110a, *et seq.*, including, but not limited to, damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

DELAWARE

FOURTEENTH CAUSE OF ACTION

VIOLATION OF THE DELAWARE CONSUMER FRAUD ACT, 6 Del. Code §§ 2513, *et seq.* (Asserted by the Delaware Subclass)

273. Plaintiff Alexandra Santana ("Plaintiff," for purposes of this Count) , individually and on behalf of the other Delaware Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

274. Equifax operating in Delaware used and employed deception, fraud, misrepresentation, and the concealment, suppression, and omission of material

facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of goods and services, in violation of 6 Del. Code § 2513(a). This includes but is not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect the Delaware Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;
- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard the Delaware Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- d. Knowingly omitting, suppressing, and concealing the inadequacy of its privacy and security protections for the Delaware Subclass Members' Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws

pertaining to the privacy and security of the Delaware Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA;

f. Failing to maintain the privacy and security of the Delaware Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the preceding paragraph, which was a direct and proximate cause of the Equifax Data Breach; and

g. Failing to disclose the Equifax Data Breach to the Delaware Subclass Members in a timely and accurate manner, in violation of 6 Del. Code § 12B-102(a).

275. As a direct and proximate result of Equifax's practices, Delaware Subclass Members suffered the injury and/or damages described herein, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

276. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. The acts caused substantial

injury to the Delaware Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

277. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Delaware Subclass Members Personal Information and that the risk of a data breach or theft was high. Equifax's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Delaware Subclass.

278. Plaintiff and Delaware Subclass Members seek damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Equifax's unlawful conduct, in an amount to be proven at trial. *See also* *Stephenson v. Capano Dev., Inc.*, 462 A.2d 1069, 1077 (Del. 1983). Plaintiff and Delaware Subclass Members also seek an order enjoining Equifax's unfair, unlawful, and/or deceptive practices, declaratory relief, attorneys' fees pursuant to 6 Del. Code §§ 2513, *et seq.*

DISTRICT OF COLUMBIA

FIFTEENTH CAUSE OF ACTION

**DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT
D.C. CODE §§ 28-3904, *ET SEQ.*
(ASSERTED BY THE DISTRICT OF COLUMBIA SUBCLASS)**

279. Plaintiff Joseph Creed Kelly ("Plaintiff," for purposes of this Count),

individually and on behalf of the other District of Columbia Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

280. As defined by D.C. Code § 28-3901, District of Columbia Subclass Members are “consumers” who purchased or received goods or services, in the form of insurance and benefits services, for personal, household, or family purposes.

281. Equifax operating in the District of Columbia engaged in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to the District of Columbia Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard District of Columbia Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of D.C. Code §§ 28-3904(a), (d), (e), (f), (h), and/or (u);
- b. Misrepresenting material facts, pertaining to the sale of goods

and services, to the District of Columbia Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of District of Columbia Subclass Members' Personal Information in violation of D.C. Code §§ 28-3904(a), (d), (e), (f), (h), and/or (u);

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for District of Columbia Subclass Members' Personal Information in violation of D.C. Code §§ 28-3904(a), (d), (e), (f), (h), and/or (u);

d. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of District of Columbia Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to District of Columbia Subclass Members in a timely and accurate

manner, in violation of D.C. Code § 28-3852(a);

f. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect District of Columbia Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

282. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

283. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard District of Columbia Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the District of Columbia Subclass.

284. As a direct and proximate result of Equifax's unlawful practices,

District of Columbia Subclass Members suffered injury and/or damages.

285. Plaintiff and District of Columbia Subclass Members seek relief under D.C. Code § 28-3905(k), including, but not limited to, restitution, injunctive relief, punitive damages, attorneys' fees and costs, and treble damages or \$1500 per violation, whichever is greater.

FLORIDA

SIXTEENTH CAUSE OF ACTION

**VIOLATION OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE
PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.*
(Asserted by the Florida Subclass)**

286. Plaintiff Trevor Dorsey ("Plaintiff," for purposes of this Count), individually and on behalf of the other Florida Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

287. Equifax operating in Florida engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1). This includes but is not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect Florida Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;

- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard Florida Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- d. Knowingly omitting, suppressing, and concealing the inadequacy of its privacy and security protections for Florida Subclass Members' Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Florida Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA, the GLBA, and Fla. Stat. § 501.171(2);
- f. Failing to maintain the privacy and security of Florida Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those

mentioned in the foregoing paragraph, which was a direct and proximate cause of the Equifax Data Breach; and

g. Failing to disclose the Equifax Data Breach to Florida Subclass Members in a timely and accurate manner, in violation of Fla. Stat. § 501.171(4).

288. As a direct and proximate result of Equifax's practices, Florida Subclass Members suffered the injury and/or damages described herein, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

289. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Florida Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

290. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Florida Subclass Members' Personal Information and that the risk of a data breach or theft was high. Equifax's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Florida Subclass Members.

291. Plaintiff and Florida Subclass Members seek actual damages under Fla. Stat. § 501.211(2), and attorneys' fees under Fla. Stat. § 501.2105(1), to be proven at trial.

292. Plaintiff and Florida Subclass Members also seek an order enjoining Equifax's unfair, unlawful, and/or deceptive practices, declaratory relief, and any other just and proper relief available under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*

GEORGIA

SEVENTEENTH CAUSE OF ACTION

GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Ga. Code Ann. §§ 10-1-370, *et seq.* (Asserted by the Georgia Subclass)

293. Plaintiff Robert Hunt ("Plaintiff," for purposes of this Count), individually and on behalf of the other Georgia Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

294. Equifax, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code Ann. § 10-1-371(5).

295. The Georgia UDTPA prohibits "deceptive trade practices," which include the "misrepresentation of standard or quality of goods or services," and

“engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.” Ga. Code Ann. § 10-1-372(a).

296. In the course of its business, Equifax willfully failed to disclose and actively concealed its grave data-security defects as discussed herein, and otherwise engaged in activities with a tendency or capacity to deceive.

297. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with accessing and storing the extremely sensitive and valuable Personal Information of Plaintiff and Georgia Subclass Members.

298. Equifax did all of this directly with respect to Plaintiff and Georgia Subclass Members, and also by way of their transactions involving goods, merchandise, and services with third parties (such as prospective creditors and creditors) who also accessed Plaintiff and Georgia Subclass Members’ extremely sensitive and valuable Personal Information in the course of those transactions.

299. For months, Equifax knew of vulnerabilities and defects in its data security systems, and vulnerabilities in key databases storing the extremely

sensitive and valuable Personal Information of Plaintiff and Georgia Subclass Members, but concealed all of that information.

300. By way of the foregoing, Equifax engaged in deceptive business practices in violation of the Georgia UDTPA.

301. Equifax also engaged in deceptive acts and practices in at least the following ways:

- a. Misrepresenting material facts (intending for others to rely upon the misrepresentations) representing that it would maintain adequate data privacy and security practices and procedures to safeguard Georgia Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts (intending for others to rely upon the misrepresentations) by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Georgia Subclass Members' Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Georgia

Subclass Members' Personal Information, with the intent that others rely on the omission, suppression, and concealment;

d. Engaging in deceptive acts and practices by failing to maintain the privacy and security of Georgia Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FRCA, the GLBA, and the Ga. Code Ann. §§ 10-1-911, *et seq.*;

e. Engaging in deceptive acts and practices by failing to disclose the data breach to Georgia Subclass Members in a timely and accurate manner, in violation of Ga. Code Ann. § 10-1-912;

f. Engaging in deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Georgia Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

302. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and Georgia Subclass

Members, regarding the security and safety of its databases and the extremely sensitive and valuable Personal Information of Plaintiff and Georgia Subclass Members.

303. Equifax intentionally and knowingly misrepresented such material facts with intent to mislead Plaintiff and Georgia Subclass Members.

304. Equifax knew or should have known that its conduct violated the Georgia UDTPA.

305. As alleged above, Equifax made material statements that were either false or misleading.

306. Equifax owed Plaintiff and Georgia Subclass Members a duty to disclose the true facts regarding data-security defects and vulnerabilities because Equifax:

- a. Possessed exclusive knowledge regarding the lack of safety of the extremely sensitive and valuable Personal Information of Plaintiff and Georgia Subclass Members;
- b. Intentionally concealed the foregoing from Plaintiff and Georgia Subclass Members; and/or

c. Made incomplete representations regarding these matters while purposefully withholding material facts from Plaintiff and Georgia Subclass Members that contradicted these representations.

307. Equifax's representations and omissions were material to Plaintiff and Georgia Subclass Members given the extreme sensitivity and value of their Personal Information.

308. Plaintiff and Georgia Subclass Members suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein.

309. Equifax had an ongoing duty to all Equifax customers, including Plaintiff and Georgia Subclass Members, to refrain from unfair and deceptive practices under the Georgia UDTPA.

310. Equifax's violations present a continuing risk to Plaintiff and Georgia Subclass Members, as well as to the general public.

311. Equifax's unlawful acts and practices complained of herein affect the public interest.

312. As a direct and proximate result of Equifax's violations of the Georgia UDTPA, Plaintiff and Georgia Subclass Members have suffered injury-in-fact and/or actual damage.

313. Plaintiff and Georgia Subclass Members seek an order enjoining Equifax’s unfair, unlawful, and/or deceptive practices, attorneys’ fees, and any other just and proper relief available under the Georgia UDTPA per Ga. Code Ann. § 10-1-373.

HAWAII

EIGHTEENTH CAUSE OF ACTION

**HAWAII UNFAIR PRACTICES AND UNFAIR
COMPETITION STATUTE, Haw. Rev. Stat. §§ 480-1, *et seq.*
(Asserted by the Hawaii Subclass)**

314. Plaintiff Bruce Pascal (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Hawaii Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

315. Hawaii Subclass Members are “consumers” as meant by Haw. Rev. Stat. § 480-1.

316. Hawaii Subclass Members purchased “goods and services” from Equifax as meant by Haw. Rev. Stat. § 480-1.

317. Hawaii Subclass Members’ purchases of goods and services from Equifax were for personal, family, and/or household purposes, as meant by Haw. Rev. Stat. § 480-1.

318. Equifax operating in Hawaii engaged in unfair methods of competition, unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass Members in violation of Haw. Rev. Stat. § 480-2(a), including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of its goods and services, to Hawaii Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Hawaii Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts, pertaining to the sale of its goods and services, to Hawaii Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Hawaii Subclass Members' Personal Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Hawaii

Subclass Members' Personal Information;

d. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Hawaii Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, and Hawaii's Privacy of Consumer Financial Information statute, (Haw. Rev. Stat. §§ 431:3A-101, *et seq.*);

e. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Hawaii Subclass Members in a timely and accurate manner, in violation of Haw. Rev. Stat. § 487N-2(a); and

f. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures

and protect Hawaii Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

319. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

320. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Hawaii Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Hawaii Subclass.

321. As a direct and proximate result of Equifax's unlawful practices, Hawaii Subclass Members suffered injury and/or damages.

322. Plaintiff and Hawaii Subclass Members seek relief under Haw. Rev. Stat. § 480-13, including, but not limited to, damages, injunctive relief, attorneys' fees and costs, and treble damages.

IDAHO

NINETEENTH CAUSE OF ACTION

**IDAHO CONSUMER PROTECTION ACT,
Idaho Code §§ 48-601, *et seq.*
(Asserted by the Idaho Subclass)**

323. Plaintiff Eileen Doten (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Idaho Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

324. Equifax’s acts and practices set forth herein are unfair and deceptive acts or practices in the conduct of trade or commerce under the Idaho Consumer Protection Act, Idaho Code §§ 48-601, *et seq.*

325. Equifax’s acts and practices as set forth above occurred in the conduct of trade or commerce.

326. Equifax is a “person” within the meaning of Idaho Code § 48-602.

327. Equifax operating in Idaho engaged in unfair methods of competition, unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Idaho Subclass Members in violation of Idaho Code § 48-603, including but not limited to the following:

- a. Passing off goods or services as those of another;

- b. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- c. Representing that goods are of a particular standard, quality, or grade when they are of another;
- d. Advertising goods or services with intent not to sell them as advertised; and
- e. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers.

328. Equifax knew, or in the exercise of due care should have known, that what it has in the past or is so representing to Idaho Subclass Members regarding its data privacy and security practices was untrue.

329. Idaho Subclass Members have suffered an ascertainable loss of money or property as a result of Equifax's unfair or deceptive acts or practices.

330. Equifax's conduct proximately caused the injuries to Plaintiff and the Idaho Subclass Members.

331. Pursuant to Idaho Code § 48-608, Plaintiff and Idaho Subclass Members ask the Court to enter injunctive relief to require Equifax to stop the unfair and deceptive conduct alleged herein, to assess damages to be proven at

trial, costs, and attorneys' fees, and to award punitive damages against Equifax for its unlawful acts and trade practices.

ILLINOIS

TWENTIETH CAUSE OF ACTION

**ILLINOIS CONSUMER FRAUD ACT,
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(Asserted by the Illinois Subclass)**

332. Plaintiff Douglas Benz ("Plaintiff," for purposes of this Count), individually and on behalf of the other Illinois Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

333. Equifax operating in Illinois engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. § 505/2, including but not limited to the following:

- a. Fraudulently advertising material facts pertaining to the goods and services to Illinois Subclass Members by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Illinois Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

- b. Misrepresenting material facts pertaining to goods and services to Illinois Subclass Members by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Subclass Members' Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Illinois Subclass Members' Personal Information with the intent that others rely on the omission, suppression, and concealment;
- d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Illinois Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. § 5/1014), Illinois laws regulating the use and disclosure of Social Security Numbers

(815 Ill. Comp. Stat § 505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. § 510/2(a));

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Equifax Data Breach to Illinois Subclass Members in a timely and accurate manner, contrary to the duties imposed by 815 Ill. Comp. Stat. § 530/10(a); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Illinois Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

334. As a direct and proximate result of Equifax's deceptive trade practices, Illinois Subclass Members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and damages, as described above.

335. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

336. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Illinois Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Illinois Subclass.

337. Plaintiff and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 505/10a, including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs.

TWENTY-FIRST CAUSE OF ACTION

**ILLINOIS UNIFORM DECEPTIVE TRADE
PRACTICES ACT,
815 Ill. Comp. Stat. §§ 510/2, *et seq.*
(Asserted by the Illinois Subclass)**

338. Plaintiff Douglas Benz ("Plaintiff," for purposes of this Count), individually and on behalf of the other Illinois Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

339. While in the course of its businesses, Equifax operating in Illinois engaged in deceptive trade practices by making false representations, including its representations that it had adequate computer systems and data security practices to protect Personal Information, when its computer systems and data security

practices were inadequate, in violation of 815 Ill. Comp. Stat. §§ 510/2(a)(5), and (7).

340. Equifax knew or should have known that its computer systems and data security practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

341. Illinois Subclass Members are likely to be damaged by Equifax's deceptive trade practices.

342. Plaintiff and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510, including, but not limited to, injunctive relief and attorney's fees.

IOWA

TWENTY-SECOND CAUSE OF ACTION

IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT, Iowa Code § 714H (Asserted by the Iowa Subclass)

343. Plaintiff Glenntavius Nolan ("Plaintiff," for purposes of this Count), individually and on behalf of the other Iowa Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

344. The Iowa Private Right of Action for Consumer Frauds Act prohibits unfair and deceptive trade practices in the sale, lease, or advertisement of a product

or service, and in the solicitation of charitable contributions. The Iowa Private Right of Action for Consumer Frauds Act's purpose is to protect consumers against these unfair and deceptive business practices and provide efficient and economical procedures to secure such protection.

345. Equifax operating in Iowa has violated the Act by engaging in the unfair and/or deceptive acts and practices described herein, which were and are intended to and did and do result in the purchase of Equifax's products and services by consumers, including Plaintiff and Iowa Subclass Members.

346. Plaintiff has provided the requisite notice to the Iowa Attorney General, which office has approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

347. As a result of Equifax's unfair and/or deceptive business practices, Plaintiff and Iowa Subclass Members have lost money or property and therefore seek their actual damages.

348. Plaintiff and Iowa Subclass Members also seek and are entitled to an order enjoining Equifax from continuing to engage in the unfair and deceptive business practices alleged herein.

KANSAS

TWENTY-THIRD CAUSE OF ACTION

**KANSAS CONSUMER PROTECTION ACT, K.S.A. §§ 50-623, *et seq.*
(Asserted by the Kansas Subclass)**

349. Plaintiff Amie Smith (“Plaintiff,” for purposes of this Court) individually and on behalf of the other Kansas Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

1. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

2. Plaintiff and Kansas Subclass Members are “consumers” as defined by K.S.A. § 50-624(b).

3. The acts and practices described herein are “consumer transactions” as defined by K.S.A. § 50-624(c).

4. Equifax is a “supplier” as defined by K.S.A. § 50-624(l).

5. The inadequacy of Equifax’s security and privacy practices and procedures was a material fact.

6. Equifax operating in Kansas engaged in acts and practices in connection with consumer transactions in violation of K.S.A. § 50-626, including but not limited to the following:

- a. Making representations, knowingly or with reason to know, that property or services have sponsorship, approval, accessories, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Making representations, knowingly or with reason to know, that, as a supplier, it has a sponsorship, approval, status, affiliation, or connection that it does not have;
- c. Making representations, knowingly or with reason to know, that property or services are of a particular standard, quality, grade, style, or model, when they are of another which differs materially from the representation;
- d. Making representations, knowingly or with reason to know, that property or services has uses, benefits or characteristics without relying upon or possessing a reasonable basis for making such representations;
- e. Making representations, knowingly or with reason to know, that use, benefit, or characteristic of property or services has been proven or otherwise substantiated without relying upon or possessing the type of proof or substantiation represented to exist; and

f. Willfully using, in any oral or written representations, exaggeration, falsehood, innuendo, or ambiguity as to a material fact.

7. Equifax engaged in acts and practices in connection with consumer transactions in violation of K.S.A. § 50-627, including but not limited to the following:

a. Entering into a consumer transaction knowing or with reason to know that Plaintiff and Kansas Subclass Members were unable to receive a material benefit from the subject of the transaction; and

b. Making a misleading statement of opinion on which Plaintiff and Kansas Subclass Members were likely to rely to their detriment.

8. Plaintiff and Kansas Subclass Members have incurred damages as a direct result of Equifax's deceptive and/or unconscionable acts and practices and are "aggrieved" as defined in K.S.A. §§ 50-634 and 636.

9. Plaintiff and Kansas Subclass Members are thus entitled to civil penalties or their actual damages, whichever is greater, as well as costs and legal fees.

10. In addition, for the benefit of the general public, Plaintiff and Kansas Subclass Members entitled to an injunction to prevent Equifax from continuing its

practices of violating the Kansas Consumer Protection Act by engaging in the acts and practices described herein.

KENTUCKY

TWENTY-FOURTH CAUSE OF ACTION

**KENTUCKY CONSUMER PROTECTION ACT,
Ky. Rev. Stat. §§ 367.110, *et seq.*
(Asserted by the Kentucky Subclass)**

11. Plaintiff Mary Hexter Moneypenny (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Kentucky Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

12. Plaintiff and Kentucky Subclass Members purchased goods and services for personal, family, and/or household purposes from Equifax.

13. Equifax operating in Kentucky engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Ky. Rev. Stat. § 367.170, including but not limited to the following:

- a. Fraudulently advertising material facts pertaining to its good and services to the Kentucky Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Kentucky Subclass Members’ Personal

Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts pertaining to goods and services to the Kentucky Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Kentucky Subclass

Members' Personal Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Kentucky Subclass Members' Personal Information;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Kentucky Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Equifax Data Breach to Kentucky Subclass Members in a timely and accurate manner, contrary to the duties imposed by Ky. Rev. Stat. § 365.732(2); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Kentucky Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

14. As a direct and proximate result of Equifax's deceptive trade practices, Kentucky Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

15. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

16. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

17. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Kentucky Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Kentucky Subclass.

18. Plaintiff and Kentucky Subclass Members seek relief under Ky. Rev. Stat. § 367.220, including, but not limited to, damages, punitive damages, restitution and/or other equitable relief, injunctive relief, and/or attorneys' fees and costs.

LOUISIANA

TWENTY-FIFTH CAUSE OF ACTION

**LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER
PROTECTION LAW, La Rev. Stat. Ann. §§ 51:1401, *et seq.*
(Asserted by the Louisiana Subclass)**

19. Plaintiff Jasmine Guess (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Louisiana Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

20. Equifax, Plaintiff, and the Louisiana Subclass Members are “persons” within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

21. Plaintiff and Louisiana Subclass Members are “consumers” within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

22. Equifax engaged in “trade” or “commerce” within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

23. The Louisiana Unfair Trade Practices and Consumer Protection Law (“Louisiana CPL”) makes unlawful “deceptive acts or practices in the conduct of any trade or commerce.” La. Rev. Stat. Ann. § 51:1405(A).

24. Equifax participated in misleading, false, or deceptive acts that violated the Louisiana CPL.

25. In the course of its business, Equifax operating in Louisiana willfully failed to disclose and actively concealed the facts discussed herein and otherwise engaged in activities with a tendency or capacity to deceive.

26. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its use and storage of consumers Personal Information.

27. Equifax knew it had not taken adequate steps to protect consumers' Personal Information from theft, as represented.

28. Equifax knew this for at least several months, but concealed all of that information.

29. Equifax was also aware that its data systems were not secure and that it had suffered multiple data breaches. Equifax concealed this information as well.

30. By failing to disclose that its computer and data systems were not secure, Equifax engaged in deceptive business practices in violation of the Louisiana CPL.

31. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the other Louisiana Subclass Members, about the true security of its computer and data systems.

32. Equifax intentionally and knowingly misrepresented material facts regarding the security of consumers' Personal Information with an intent to mislead Plaintiff and Louisiana Subclass Members.

33. Equifax knew or should have known that its conduct violated the Louisiana CPL.

34. As alleged above, Equifax made material statements about the safety and security of Personal Information that were either false or misleading.

35. Equifax owed Louisiana Subclass Members a duty to disclose the true lack of security of its computer and data systems because Equifax:

- a. Possessed exclusive knowledge that it valued profits over data security;
- b. Intentionally concealed the foregoing from Plaintiffs and the Louisiana Subclass; and/or
- c. Made incomplete representations about the security and integrity of its computer and data systems generally, and its prior data breaches in particular, while purposefully withholding material facts from Plaintiffs and the Louisiana Subclass that contradicted these representations.

36. Equifax's fraudulent representations were material to Plaintiffs and the Louisiana Subclass.

37. Plaintiffs and Louisiana Subclass Members suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein, including time and expenses associated with securing their identities from theft, including costs to implement and maintain credit freezes and identity theft monitoring and protection.

38. Equifax had an ongoing duty to all Louisiana Subclass Members under the Louisiana CPL to refrain from unfair and deceptive practices. The Subclass Members suffered ascertainable loss in the form of out-of-pocket costs and loss of time as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

39. Equifax's violations present a continuing risk to the Louisiana Subclass. Equifax's unlawful acts and practices complained of herein affect the public interest.

40. As a direct and proximate result of Equifax's violations of the Louisiana CPL, Plaintiffs and Louisiana Subclass Members have suffered injury-in-fact and/or actual damage.

41. Pursuant to La. Rev. Stat. Ann. § 51:1409, Plaintiff and Louisiana Subclass Members seek to recover actual damages in an amount to be determined at trial; treble damages for Equifax’s knowing violations of the Louisiana CPL; an order enjoining Equifax’s unfair, unlawful, and/or deceptive practices; declaratory relief; attorneys’ fees; and any other just and proper relief available under La. Rev. Stat. Ann. § 51:1409.

MAINE

TWENTY-SIXTH CAUSE OF ACTION

**MAINE UNFAIR TRADE PRACTICES ACT,
5 Me. Rev. Stat. §§ 205, 213, *et seq.*
(Asserted by the Maine Subclass)**

42. Plaintiff Kathleen Lyons (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Maine Subclass members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

43. Plaintiff and Maine Subclass Members purchased goods and/or services for personal, family, and/or household purposes from Equifax.

44. Plaintiff sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) on October 10, 2017.

45. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including but not limited to the following:

- a. Misrepresenting and fraudulently advertising material facts pertaining to goods and services to the Maine Class by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Maine Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts pertaining to goods and services to the Maine Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Maine Subclass Members' Personal Information;
- c. Omitting, suppressing and concealing the material facts of the inadequacy of the privacy and security protections for the Maine Subclass Members' Personal Information;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Maine

e. Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the Maine Insurance Information and Privacy Protection Act (Me. Rev. Stat. 24-A, § 2215(1)).

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Equifax Data Breach to Maine Subclass Members in a timely and accurate manner, contrary to the duties imposed by 10 Me. Rev. Stat. § 1348(1);

g. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Maine Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft

46. As a direct and proximate result of Equifax's deceptive trade practices, Maine Subclass Members suffered an ascertainable loss of money or

47. property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

48. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Maine Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

49. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Maine Subclass Members' Personal Information and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maine Subclass.

50. Maine Subclass Members seek relief under 5 Me. Rev. Stat. §213, including, not limited to, damages, restitution, injunctive relief, and/or attorneys' fees and costs.

TWENTY-SEVENTH CAUSE OF ACTION

**MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT,
10 Me. Rev. Stat. §§ 1212, *et seq.*
(Asserted by the Maine Subclass)**

51. Plaintiff Kathleen Lyons (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Maine Subclass members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

52. Equifax operating in Maine engaged in deceptive trade practices by making false representations, including its representations that it had adequate computer systems and data security practices to protect Personal Information, when its computer systems and data security practices were inadequate, in violation of 10 Me. Rev. Stat. §§1212(E),(G), (I), and (L).

53. Equifax knew or should have known that its computer systems and data security practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

54. Maine Subclass Members are likely to be damaged by Equifax’s deceptive trade practices.

55. Plaintiff and Maine Subclass Members seek relief under 10 Me. Rev. Stat. §1213, including, but not limited to, injunctive relief and attorney’s fees.

MARYLAND

TWENTY-EIGHTH CAUSE OF ACTION

**MARYLAND CONSUMER PROTECTION ACT,
MD. Code Ann., Com. Law §§ 13-301, *et seq.*
(Asserted by the Maryland Subclass)**

56. Plaintiff Lisa Tyree (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Maryland Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

57. Maryland Subclass Members are “consumers” as meant by Md. Code Ann., Com. Law § 13-101.

58. The goods and services that are the subject of this complaint are “consumer goods” and/or “consumer services” as meant by Md. Code Ann., Com. Law § 13-101.

59. The unlawful trade practices, misrepresentations, and omissions described herein did not constitute “professional services” on the part of Equifax.

60. Equifax operating in Maryland engaged in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of its goods and services in violation of Md. Code Ann., Com. Law § 13-301, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of its goods and services, to Maryland Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Maryland Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Md. Code Ann., Com. Law §§ 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);
- b. Misrepresenting material facts, pertaining to the sale of its goods and services, to Maryland Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Maryland Subclass Members' Personal Information in violation of Md. Code Ann., Com. Law §§ 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Maryland Subclass Members' Personal Information in violation of Md. Code Ann., Com. Law §§ 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

- d. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Maryland Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, Maryland's Privacy of Consumer Financial and Health Information regulations (Md. Code Regs. §§ 31.16.08.01, *et seq.*); Maryland's data breach statute (Md. Code Ann., Com. Law § 14-3503), and Maryland's Social Security Number Privacy Act (Md. Code Ann., Com. Law §§ 14-3401, *et seq.*);
- e. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Maryland Subclass Members in a timely and accurate manner, in violation of Md. Code Com. Law § 14-3504(b)(3); and
- f. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures

g. and protect Maryland Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

61. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Maryland Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

62. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Maryland Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maryland Subclass.

63. As a direct and proximate result of Equifax's unlawful practices, Maryland Subclass Members suffered injury and/or damages.

64. Plaintiff and Maryland Subclass Members seek relief under Md. Code Ann., Com. Law § 13-408, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs.

MASSACHUSETTS

TWENTY-NINTH CAUSE OF ACTION

MASSACHUSETTS CONSUMER PROTECTION ACT

MASS. Gen. Laws Ann. ch. 93A, §§ 1, *et seq.*

(ASSERTED BY THE MASSACHUSETTS SUBCLASS))

65. Plaintiff Jaclyn Belland (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Massachusetts Subclass members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

66. Plaintiff sent a demand for relief on behalf of the Massachusetts Subclass pursuant to Mass. Gen. Laws Ann. ch. 93A § 9(3) on October 10, 2017.

67. Equifax operates in “trade or commerce” as meant by Mass. Gen. Laws Ann. ch. 93A, § 1.

68. Equifax operating in Massachusetts engaged in deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a), including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to Massachusetts Subclass Members by representing that

it would maintain adequate data privacy and security practices and procedures to safeguard Massachusetts Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of goods and services, to Massachusetts Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Massachusetts Subclass Members' Personal Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Massachusetts Subclass Members' Personal Information;

d. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Massachusetts Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA, the GBLA, the

Massachusetts Right of Privacy statute (Mass. Gen. Laws Ann. ch. 214, § 1B), and the Massachusetts data breach statute (Mass. Gen. Laws Ann. ch. 93H, § 3(a));

e. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Massachusetts Class Members in a timely and accurate manner, in violation of Mass. Gen. Laws Ann. ch. 93H, § 3(a);

f. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Massachusetts Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

69. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Massachusetts Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within the penumbra of common law, statutory, or other established concepts of unfairness. Equifax knew or should have known that their computer systems and data security practices were inadequate to

safeguard Massachusetts Subclass Members' Personal Information and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Massachusetts Subclass.

70. As a direct and proximate result of Equifax's unlawful practices, Massachusetts Subclass Members suffered injury and/or damages.

71. Plaintiff and Massachusetts Subclass Members seek relief under Mass. Gen. Laws Ann. ch. 93A, § 9, including, but not limited to, actual damages, double or treble damages, injunctive and/or other equitable relief, and/or attorneys' fees and costs.

MICHIGAN

THIRTIETH CAUSE OF ACTION

MICHIGAN CONSUMER PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.903, *et seq.* (Asserted by the Michigan Subclass)

72. Plaintiff Nicole Walker ("Plaintiff," for purposes of this Count), individually and on behalf of the other Michigan Subclass Members, repeats and repeats and alleges Paragraphs 1-160, as if fully alleged herein.

73. Equifax operating in Michigan engaged in unfair, unconscionable, and deceptive methods, acts, and practices in the conduct of trade and commerce, including representing that its good and services had characteristics that they did not, representing that its goods and services were of a particular standard when they were not, and advertising its goods and services with intent not to dispose of them as advertised, in violation of Mich. Comp. Laws Ann. § 445.903(1). This includes but is not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect Michigan Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;
- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard Michigan Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

- d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for Michigan Subclass Members' Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Michigan Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA;
- f. Failing to maintain the privacy and security of Michigan Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Equifax Data Breach; and
- g. Failing to disclose the Equifax Data Breach to Michigan Subclass Members in a timely and accurate manner, in violation of the duties imposed by Mich. Comp. Laws Ann. § 445.72(1).

74. As a direct and proximate result of these practices, Michigan Subclass Members suffered injuries to legally protected interests, as described above,

including but not limited to their legally protected interest in the confidentiality and privacy of their Personal Information, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

75. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Michigan Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within the penumbra of common law, statutory, or other established concepts of unfairness.

76. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Michigan Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Michigan Subclass Members.

77. Plaintiff and Michigan Subclass Members seek injunctive relief to enjoin Equifax from continuing its unfair and deceptive acts; monetary relief against Equifax measured as the greater of (a) actual damages in an amount to be

determined at trial and (b) statutory damages in the amount of \$250 for Plaintiff and each Michigan Subclass Member; reasonable attorneys' fees; and any other just and proper relief available under Mich. Comp. Laws Ann. § 445.911.

MINNESOTA

THIRTY-FIRST CAUSE OF ACTION

**MINNESOTA CONSUMER FRAUD ACT,
Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.*
(Asserted by the Minnesota Subclass)**

78. Plaintiff Mike Spicer ("Plaintiff," for purposes of this Count), individually and on behalf of the other Minnesota Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

79. Equifax's goods and services are "merchandise" as defined by Minn. Stat. § 325F.68.

80. Equifax operating in Minnesota engaged in unlawful practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of services in violation of Minn. Stat. § 325F.69, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to the Minnesota Subclass by representing that it would maintain adequate data privacy and security practices and procedures

to safeguard Minnesota Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of goods and services, to the Minnesota Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Minnesota Subclass

Members' Personal Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Minnesota Subclass Members' Personal Information;

d. Engaging in unlawful and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to Minnesota Subclass Members in a timely and accurate manner, in violation of Minn. Stat. § 325E.61(1)(a); and

e. Engaging in unlawful and deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Minnesota Subclass Members'

Personal Information from further unauthorized disclosure, release, data breaches, and theft.

81. The above unlawful and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Minnesota Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

82. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Minnesota Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the abovenamed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Minnesota Subclass.

83. As a direct and proximate result of Equifax's unlawful practices, Minnesota Subclass Members suffered injury and/or damages.

84. Plaintiff and Minnesota Subclass Members seek relief under Minn. Stat. § 8.31, including, but not limited to, damages, injunctive and/or other equitable relief, and attorneys' fees and costs.

THIRTY-SECOND CAUSE OF ACTION

**MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
Minn. Stat. §§ 325D.43, *et seq.*
(Asserted by the Minnesota Subclass)**

85. Plaintiff Mike Spicer (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Minnesota Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

86. Equifax operating in Minnesota engaged in deceptive practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of its goods and services in violation of Minn. Stat. § 325D.44, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to the Minnesota Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Minnesota Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Minn. Stat. §§ 325D.44(5), (7), (9), and (13);
- b. Misrepresenting material facts, pertaining to the sale of goods and services, to the Minnesota Subclass by representing that it did and would comply with the requirements of relevant federal and state laws

pertaining to the privacy and security of Minnesota Subclass Members' Personal Information in violation of Minn. Stat. §§ 325D.44(5), (7), (9), and (13);

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Minnesota Subclass Members' Personal Information in violation of Minn. Stat. §§ 325D.44(5), (7), (9), and (13);

d. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of Minnesota Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in unlawful and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to Minnesota Subclass Members in a timely and accurate manner, in violation of Minn. Stat. § 325E.61(1)(a); and

f. Engaging in unlawful and deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Minnesota Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

87. The above unlawful and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Minnesota Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

88. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Minnesota Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the abovenamed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Minnesota Subclass.

89. As a direct and proximate result of Equifax's unlawful and deceptive trade practices, the Equifax Data Breach affected thousands of Minnesotans. Even beyond these Minnesotans, the impact on the public is widespread, including the long-term impairment of credit scores, fraudulent tax filings, and national security implications.

90. As a direct and proximate result of Equifax's unlawful practices, Minnesota Subclass Members suffered injury and/or damages.

91. Plaintiff and Minnesota Subclass Members seek relief under Minn. Stat. § 325D.45, including, but not limited to, injunctive relief and attorneys' fees and costs, and also seek relief under Minn. Stat. Ann. § 8.31, including, but not limited to, damages.

MISSOURI

THIRTY-THIRD CAUSE OF ACTION

MISSOURI MERCHANDISE PRACTICES ACT, Mo. Rev. Stat. §§ 407.010, *et seq.* (Asserted by the Missouri Subclass)

92. Plaintiff Kayla Ferrel ("Plaintiff," for purposes of this Count), individually and on behalf of the other Missouri Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

93. Plaintiff and Missouri Subclass Members purchased “merchandise” in “trade” or “commerce” as meant by Mo. Rev. Stat. § 407.010 when they purchased Equifax’s goods and services for personal, family, and/or household purposes.

94. Equifax operating in Missouri engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of its goods and services in violation of Mo. Rev. Stat. § 407.020(1), including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of its goods and services, to the Missouri Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Missouri Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts, pertaining to the sale of goods and services, to the Missouri Subclass by representing that it did and would comply with the requirements of relevant federal and state laws

pertaining to the privacy and security of Missouri Subclass Members' Personal Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Missouri Subclass Members' Personal Information;

d. Engaging in unfair acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Missouri Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in unlawful and deceptive acts and practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Missouri Subclass Members in a timely and accurate manner, in violation of Mo. Rev. Stat. § 407.1500(2)(1)(a); and

f. Engaging in unlawful and deceptive acts and practices with respect to the sale of its goods and services by failing to take proper

action following the Equifax Data Breach to enact adequate privacy and security measures and protect Missouri Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

95. The above unlawful and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Missouri Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

96. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Missouri Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Missouri Subclass.

97. As a direct and proximate result of Equifax's unlawful practices, Missouri Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

98. Plaintiff and Missouri Subclass Members seek relief under Mo. Rev. Stat. § 407.025, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys’ fees and costs.

MONTANA

THIRTY-FOURTH CAUSE OF ACTION

**MONTANA UNFAIR TRADE PRACTICES AND CONSUMER
PROTECTION ACT, MCA §§ 30-14-101, *et seq.*
(Asserted by the Montana Subclass)**

99. Plaintiff Terry Ford (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Montana Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

100. Plaintiff and Montana Subclass Members are “consumers” as meant by MCA§ 30-14-102.

101. Equifax offered its goods and services in “trade” and “commerce,” as meant by MCA § 30-14-102, for personal, family, and/or household purposes.

102. Equifax operating in Montana engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of its goods and services to Montana Subclass Members in violation MCA § 30-14-103, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to Montana Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Montana Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts, pertaining to the sale of goods and services, to the Montana Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Montana Subclass Members' Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Montana Subclass Members' Personal Information;
- d. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of Montana Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax

Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

- e. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to Montana Subclass Members in a timely and accurate manner, in violation of MCA§ 30-14-1704(1); and
- f. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Montana Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

103. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Montana Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

104. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Montana Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Montana Subclass.

105. As a direct and proximate result of Equifax's deceptive acts and practices, Montana Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

106. Plaintiff and Montana Subclass Members seek relief under MCA § 30-14-133, including, but not limited to, injunctive relief, other equitable relief, actual damages or \$500 per Subclass Member, whichever is greater, treble damages, and attorneys' fees and costs.

NEBRASKA

THIRTY-FIFTH CAUSE OF ACTION

**NEBRASKA CONSUMER PROTECTION ACT,
Neb. Rev.Stat. §§ 59-1601, *et seq.*
(Asserted by the Nebraska Subclass)**

107. Plaintiff Eric Barber (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Nebraska Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

108. Equifax engages in “trade and commerce,” as meant by Neb. Rev. Stat. § 59-1601, by selling goods and services.

109. Equifax operating in Nebraska engaged in unfair and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of products and services in violation of Neb. Rev. Stat. § 59-1602, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to Nebraska Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Nebraska Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting
- c. Misrepresenting material facts, pertaining to the sale of goods and services, to Nebraska Subclass Members by representing that it did

and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nebraska Subclass Members' Personal Information;

d. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Nebraska Subclass Members' Personal Information;

e. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of Nebraska Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

f. Engaging in unlawful and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to Nebraska Subclass Members in a timely and accurate manner, in violation of Neb. Rev. Stat. § 87-803(1); and

g. Engaging in unlawful and deceptive acts and practices with respect to the sale of goods and services by failing to take proper

action following the Equifax Data Breach to enact adequate privacy and security measures and protect Nebraska Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

110. The above unlawful and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Nebraska Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

111. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Nebraska Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nebraska Subclass.

112. As a direct and proximate result of Equifax's unlawful practices, Nebraska Subclass Members suffered injury and/or damages.

113. Plaintiff and Nebraska Subclass Members seek relief under Neb. Rev. Stat. § 59-1609, including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs.

THIRTY-SIXTH CAUSE OF ACTION

**NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
Neb. Rev. Stat. §§ 87-301, *et seq.*
(Asserted by the Nebraska Subclass)**

114. Plaintiff Eric Barber ("Plaintiff," for purposes of this Count), individually and on behalf of the other Nebraska Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

115. Equifax operating in Nebraska engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of Neb. Rev. Stat. § 87-302 including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to Nebraska Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Nebraska Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, in violation of Neb. Rev. Stat. §§ 87-302 (5), (7), (9), and (15);

- b. Misrepresenting material facts, pertaining to the sale of goods and services, to Nebraska Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nebraska Subclass Members' Personal Information, in violation of Neb. Rev. Stat. §§ 87-302 (5), (7), (9), and (15);
- c. Omitting, suppressing, and concealed the material fact of the inadequacy of the privacy and security protections for Nebraska Subclass Members' Personal Information in violation of Neb. Rev. Stat. §§ 87-302(5), (7), (9), and (15);
- d. Engaging in deceptive trade practices with respect to the sale of goods and services by failing to maintain the privacy and security of Nebraska Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These deceptive trade practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;
- e. Engaging in deceptive trade practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to

Nebraska Subclass Members in a timely and accurate manner, in violation of Neb. Rev. Stat. § 87-803(1); and

f. Engaging in deceptive trade practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Nebraska Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

116. The above deceptive trade practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Nebraska Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

117. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Nebraska Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nebraska Subclass.

118. As a direct and proximate result of Equifax's unlawful practices, Nebraska Subclass Members suffered injury and/or damages.

119. Plaintiff and Nebraska Subclass Members seek relief under Neb. Rev. Stat. § 87-303, including, but not limited to, injunctive relief, other equitable relief, and attorneys' fees and costs.

NEVADA

THIRTY-SEVENTH CAUSE OF ACTION

**NEVADA DECEPTIVE TRADE PRACTICES ACT,
Nev. Rev. Stat. Ann. §§ 598.0915, *et seq.*
(Asserted by the Nevada Subclass)**

120. Plaintiff Katherine Timmons ("Plaintiff," for purposes of this Count), individually and on behalf of the other Nevada Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

121. In the course of its businesses, Equifax operating in Nevada engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of its goods and services in violation of Nev. Rev. Stat. Ann. § 598.0915, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of its goods and services, to the Nevada Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Nevada Subclass Members' Personal

Information from unauthorized disclosure, release, data breaches, and theft, in violation of Nev. Rev. Stat. Ann. §§ 598.0915(5), (7), (9), and (15);

b. Misrepresenting material facts, pertaining to the sale of its goods and services, to the Nevada Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nevada Subclass Members' Personal Information, in violation of Nev. Rev. Stat. Ann. §§ 598.0915(5), (7), (9), and (15);

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Nevada Subclass Members' Personal Information, in violation of Nev. Rev. Stat. Ann. §§ 598.0915(5), (7), (9), and (15);

d. Engaging in deceptive trade practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Nevada Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not

limited to the FCRA, the GLBA, and the Nevada data breach statute (Nev. Rev. Stat. Ann. § 603A.210).

e. Engaging in deceptive trade practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Nevada Subclass Members in a timely and accurate manner, in violation of Nev. Rev. Stat. Ann. § 603A.220(1); and

f. Engaging in deceptive trade practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Nevada Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

122. The above unlawful and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Nevada Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

123. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Nevada Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's

actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nevada Subclass.

124. As a direct and proximate result of Equifax's deceptive practices, Nevada Subclass Members suffered injury and/or damages.

125. Plaintiff and Nevada Subclass Members seek relief under Nev. Rev. Stat. Ann. § 41.600, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

NEW HAMPSHIRE

THIRTY-EIGHTH CAUSE OF ACTION

**NEW HAMPSHIRE CONSUMER PROTECTION ACT,
N.H.R.S.A. §§ 358-A, *et seq.*
(Asserted by the New Hampshire Subclass)**

126. Plaintiff Andrew Sheppe ("Plaintiff," for purposes of this Count), individually and on behalf of the other New Hampshire Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

127. The New Hampshire Consumer Protection Act makes it unlawful for "any person to use any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce." N.H.R.S.A. § 358-A:2.

128. Equifax is a “person” under the New Hampshire Consumer Protection Act and its marketing and selling of its goods and services is “trade” and “commerce” within the meaning of the Act.

129. Equifax operating in New Hampshire engaged in unfair or deceptive acts or practices in violations of N.H.R.S.A. § 358-A:2 in the conduct of trade or commerce, including but not limited to:

- a. Representing that its goods and services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. Representing that its goods and services are of a particular standard, quality or grade when they are of another; and
- c. Advertising its goods and services with intent not to sell them as advertised.

130. Furthermore, N.H.R.S.A. § 638:6, entitled “Deceptive Business Practices,” declares a person guilty of a class B misdemeanor if, in the course of business, he:

- a. Sells, offers or exposes for sale adulterated or mislabeled commodities; or

b. Makes a false or misleading statement in any advertising addressed to the public for the purpose of promoting the purchase or sale of property or services.

131. Equifax's violations of N.H.R.S.A. § 638:6 constitute independent violations of the Act.

132. Equifax violated the Act by making representations and omissions as described above when it knew, or should have known, that the representations and omissions were unfair and/or deceptive.

133. Equifax's unfair and/or deceptive acts or practices as described herein caused and continue to cause substantial injury to Plaintiff and New Hampshire Subclass Members.

134. Plaintiff and New Hampshire Subclass Members have suffered injury in fact and lost money as a result of Equifax's unfair and/or deceptive conduct.

135. Thus, pursuant to N.H.S.R.A. §§ 358-A:10 and 358-A:10-a, Plaintiff and New Hampshire Subclass Members are entitled to damages and equitable relief.

136. As provided by N.H.R.S.A. § 358-A:10-a, Plaintiff may bring this class action under N.H.R.S.A. § 358-A:10 because Equifax has continuously

engaged in uniformly unfair and/or deceptive acts or practices throughout the relevant period, which have caused similar injury to the other New Hampshire Subclass Members.

137. Moreover, because Equifax’s unfair and/or deceptive conduct was willful or knowing, Plaintiff and New Hampshire Subclass Members are entitled to treble damages.

138. Plaintiff and New Hampshire Subclass Members are also entitled to recover costs and reasonable fees.

NEW JERSEY

THIRTY-NINTH CAUSE OF ACTION

**NEW JERSEY CONSUMER FRAUD ACT,
N.J. Stat. Ann. §§ 56:8-1, *et seq.*
(Asserted by the New Jersey Subclass)**

139. Plaintiff Carlos Martinho (“Plaintiff,” for purposes of this Count), individually and on behalf of the other New Jersey Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

140. Equifax sells “merchandise,” as meant by N.J. Stat. Ann. § 56:8-1, by offering its goods and services to the public.

141. Equifax operating in New Jersey engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression,

and omission of material facts with respect to the sale and advertisement of its goods and services in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of its goods and services, to the New Jersey Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard New Jersey Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts, pertaining to the sale of its goods and services, to the New Jersey Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New Jersey Subclass Members' Personal Information;
- c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for New Jersey Subclass Members' Personal Information with the intent that others rely on the omission, suppression, and concealment;

d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of New Jersey Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in unconscionable and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to New Jersey Subclass Members in a timely and accurate manner, in violation of N.J. Stat. Ann. § 56:8-163(a); and

f. Engaging in unconscionable and deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect New Jersey Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

142. The above unlawful and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and New Jersey Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

143. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard New Jersey Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Jersey Subclass.

144. As a direct and proximate result of Equifax's unconscionable or deceptive acts and practices, New Jersey Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

145. Plaintiff and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

NEW MEXICO

FORTIETH CAUSE OF ACTION

**NEW MEXICO UNFAIR PRACTICES ACT,
N.M. Stat. Ann. §§ 57-12-2, *et seq.*
(Asserted by the New Mexico Subclass)**

146. Plaintiff Dean Armstrong (“Plaintiff,” for purposes of this Count), individually and on behalf of the other New Mexico Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein..

147. Equifax operating in New Mexico engaged in unconscionable, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of its goods and services in violation of N.M. Stat. Ann. § 57-12-3, including but not limited to the following:

- a. Knowingly misrepresenting material facts, pertaining to the sale of its goods and services, to New Mexico Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard New Mexico Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft;

- b. Knowingly misrepresenting material facts, pertaining to the sale of its goods and services, to New Mexico Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New Mexico Subclass Members' Personal Information;
- c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for New Mexico Subclass Members' Personal Information;
- d. Engaging in unfair, unconscionable, and deceptive acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of New Mexico Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unconscionable, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;
- e. Engaging in unfair, unconscionable, and deceptive acts and practices with respect to the sale of goods and services by failing

to disclose the Equifax Data Breach to New Mexico Subclass Members in a timely and accurate manner; and

- f. Engaging in unfair, unconscionable, and deceptive acts and practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect New Mexico Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

148. The above unfair, unconscionable, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and New Mexico Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

149. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard New Mexico Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair, unconscionable, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Mexico Subclass.

150. As a direct and proximate result of Equifax's unfair, unconscionable, and deceptive acts and practices, New Mexico Subclass Members suffered a loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

151. Plaintiff and New Mexico Subclass Members seek relief under N.M. Stat. Ann. § 57-12-10, including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs, as well as treble damages or \$300 per New Mexico Subclass Member, whichever is greater.

NEW YORK

FORTY-FIRST CAUSE OF ACTION

**NEW YORK GENERAL BUSINESS LAW,
N.Y. Gen. Bus. Law §§ 349, *et seq.*
(Asserted by the New York Subclass)**

152. Plaintiff Kyoko Yamamoto ("Plaintiff," for purposes of this Count), individually and on behalf of the other New York Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

153. Equifax operating in New York engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing

of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- a. Misrepresenting and fraudulently advertising material facts, pertaining to the sale and/or furnishing of its goods and services, to the New York Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard New York Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts, pertaining to the sale and/or furnishing of its goods and services, to the New York Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New York Subclass Members' Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for New York Subclass Members' Personal Information;
- d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of New York

Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Equifax Data Breach to New York Subclass Members in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect New York Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

154. As a direct and proximate result of Equifax's deceptive trade practices, New York Subclass Members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

155. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

156. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard New York Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New York Subclass.

157. Plaintiff and New York Subclass Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

NORTH CAROLINA

FORTY-SECOND CAUSE OF ACTION

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT, N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.* (Asserted by the North Carolina Subclass)

158. Plaintiff Nancy Dubin ("Plaintiff," for purposes of this Count),

individually and on behalf of the other North Carolina Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

159. Equifax's sale, advertising, and marketing of its goods and services affected commerce, as meant by N.C. Gen. Stat. Ann. § 75-1.1.

160. Equifax operating in North Carolina engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of N.C. Gen. Stat. Ann. § 75-1.1, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to the North Carolina Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard North Carolina Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts, pertaining to the sale of its good and services, to the North Carolina Subclass by representing that it did and would comply with the requirements of relevant federal and state

laws pertaining to the privacy and security of North Carolina Subclass Members' Personal Information;

- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for North Carolina Subclass Members' Personal Information;
- d. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of North Carolina Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, and the North Carolina Identity Theft Protection Act (N.C. Gen. Stat. Art. 2A §§ 75-60, *et seq.*);
- e. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to North Carolina Subclass Members in a timely and accurate manner, in violation of N.C. Gen. Stat. Ann. § 76-65(a); and

f. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect North Carolina Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

161. The above unfair, unlawful, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and North Carolina Subclass Members that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

162. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard North Carolina Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the abovenamed unfair, unconscionable, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Carolina Subclass.

163. As a direct and proximate result of Equifax's unfair, unconscionable, and deceptive acts and practices, North Carolina Subclass Members suffered injury and/or damages.

164. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. Ann. §§ 75-16 and 75-16.1, including, but not limited to, injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

NORTH DAKOTA

FORTY-THIRD CAUSE OF ACTION

NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT, N.D. Cent. Code §§ 51-10-01, *et seq.* (Asserted by the North Dakota Subclass)

165. Plaintiff Christina Martell ("Plaintiff," for purposes of this Count), individually and on behalf of the other North Dakota Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

166. Equifax sells and advertises "merchandise," as meant by N.D. Cent. Code § 51-15-01, in the form of its goods and services.

167. Equifax operating in North Dakota engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in

violation of N.D. Cent. Code § 51-15-01, including but not limited to the following:

- a. Misrepresenting material facts (intending for others to rely upon the misrepresentations), pertaining to the sale of goods and services, to the North Dakota Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard North Dakota Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts (intending for others to rely upon the misrepresentations), pertaining to the sale of goods and services, to the North Dakota Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of North Dakota Subclass Members' Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for North Dakota Subclass Members' Personal Information, with the intent that others rely on the omission, suppression, and concealment;

d. Engaging in deceptive acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of North Dakota Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to North Dakota Subclass Members in a timely and accurate manner, in violation of N.D. Cent. Code § 51-30-02; and

f. Engaging in deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect North Dakota Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

168. The above deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to

Plaintiff and North Dakota Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

169. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard North Dakota Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Dakota Subclass.

170. As a direct and proximate result of Equifax's deceptive acts and practices, Equifax acquired money or property from North Dakota Subclass Members.

171. Plaintiff and North Dakota Subclass Members seek relief under N.D. Cent. Code Ann. § 51-15-09, including, but not limited to, injunctive relief, damages, restitution, treble damages, and attorneys' fees and costs.

OHIO
FORTY-FOURTH CAUSE OF ACTION
OHIO CONSUMER SALES PRACTICES ACT,
Ohio Rev. Code §§ 1345.01, *et seq.*
(Asserted by the Ohio Subclass)

172. Plaintiff David White (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Ohio Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

173. Equifax operating in Ohio engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.01(A) and (B), including but not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect the Ohio Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;
- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures

- d. to safeguard the Ohio Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- e. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for the Ohio Subclass Members' Personal Information;
- f. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Ohio Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA;
- g. Failing to maintain the privacy and security of the Ohio Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Equifax Data Breach; and
- h. Failing to disclose the Equifax Data Breach to the Ohio Subclass Members in a timely and accurate manner, in violation of the duties imposed by Ohio Rev. Code § 1349.19(B).

174. As a direct and proximate result of Equifax's practices, the Ohio Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

175. The above unfair and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Ohio Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

176. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Ohio Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

177. Pursuant to Ohio Rev. Code § 1345.09, Plaintiff and the Ohio Subclass Members seek an order enjoining Equifax's unfair and/or deceptive acts or practices, actual damages – trebled (to be proven at the time of trial), attorneys' fees and costs, and any other just and proper relief, to the extent available under the Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01, *et seq.*

FORTY-FIFTH CAUSE OF ACTION

**OHIO DECEPTIVE TRADE PRACTICES ACT,
Ohio Rev. Code §§ 4165.01, *et seq.*
(Asserted by the Ohio Subclass)**

178. Plaintiff David White (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Ohio Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

179. Equifax operating in Ohio engaged in deceptive trade practices in the course of its business and vocation, including representing that its services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised in violation of Ohio Rev. Code § 4165.02(A). This includes but is not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect the Ohio Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;
- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;

- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard the Ohio Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for the Ohio Subclass Members' Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Ohio Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA;
- f. Failing to maintain the privacy and security of the Ohio Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Equifax Data Breach; and

g. Failing to disclose the Equifax Data Breach to the Ohio Subclass Members in a timely and accurate manner, in violation of the duties imposed by Ohio Rev. Code § 1349.19(B).

180. As a direct and proximate result of Equifax's practices, Ohio Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

181. The above unfair and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Ohio Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

182. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Ohio Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

183. Pursuant to Ohio Rev. Code §§4165.01, Plaintiff and Ohio Subclass Members seek an order enjoining Equifax's unfair and/or deceptive acts or

practices, actual damages – trebled (to be proven at the time of trial), attorneys’ fees and costs, and any other just and proper relief, to the extent available under the Ohio Deceptive Trade Practices Act, Ohio Rev. Code §§ 4165.01, *et seq.*

OKLAHOMA

FORTY-SIXTH CAUSE OF ACTION

**OKLAHOMA CONSUMER PROTECTION ACT,
Okla. Stat. tit. 15, §§ 751, *et seq.*
(Asserted by the Oklahoma Subclass)**

184. Plaintiff Darin Marion (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Oklahoma Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

185. Plaintiff and Oklahoma Subclass Members purchased “merchandise,” as meant by Okla. Stat. tit. 15, § 752, in the form of Equifax’s goods and services.

186. Plaintiff’s and Oklahoma Subclass Members’ purchases of goods and services from Equifax constituted “consumer transactions” as meant by Okla. Stat. tit. 15, § 752.

187. Equifax operating in Oklahoma engaged in unlawful, unfair, and deceptive trade practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the

services purchased by the Oklahoma Subclass in violation of Okla. Stat.. tit. 15, § 753, including but not limited to the following:

- a. Knowingly, or with reason to know, misrepresenting material facts pertaining to the sale of its goods and services to Oklahoma Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Oklahoma Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Okla. Stat. tit. 15, §§ 753(5) and (8);
- b. Knowingly, or with reason to know, misrepresenting material facts pertaining to the sale of its goods and services to Oklahoma Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Oklahoma Subclass Members' Personal Information in violation of Okla. Stat. tit. 15, §§ 753(5) and (8);
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Oklahoma Subclass Members' Personal Information in violation of Okla. Stat. tit. 15, §§ 753(5) and (8);

d. Engaging in unfair, unlawful, and deceptive trade practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Oklahoma Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FRCA and the GLBA;

e. Engaging in unlawful, unfair, and deceptive trade practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Oklahoma Subclass Members in a timely and accurate manner, in violation of 24 Okla. Stat. Ann. § 163(A); and

f. Engaging in unlawful, unfair, and deceptive trade practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Oklahoma Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

188. The above unlawful, unfair, and deceptive trade practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Oklahoma Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

189. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Oklahoma Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Oklahoma Subclass Members.

190. As a direct and proximate result of Equifax's deceptive acts and practices, the Oklahoma Subclass Members suffered injury and/or damages.

191. Plaintiff and Oklahoma Subclass Members seek relief under Okla. Stat. Ann. tit. 15, § 761.1, including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs.

OREGON

FORTY-SEVENTH CAUSE OF ACTION

**OREGON UNLAWFUL TRADE PRACTICES ACT,
Or. Rev. Stat. §§ 646.608, *et seq.*
(Asserted by the Oregon Subclass)**

192. Plaintiff Patricia Baxter (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Oregon Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

193. Equifax operating in Oregon engaged in deceptive trade practices in the course of its business and occupation, including by representing that its goods and services had characteristics that they did not have, representing that its goods and services were of a particular standard or quality when they were not, advertising its goods and services with intent not to sell them as advertised, and engaging in other unfair and deceptive conduct in trade or commerce, in violation of Or. Rev. Stat. §§ 646.608(1)(e), (g), and (u).

194. This includes but is not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect Oregon Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;

- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard the Oregon Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for Oregon Subclass Members' Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Oregon Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA;
- f. Failing to maintain the privacy and security of Oregon Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those

mentioned in the aforementioned paragraph, directly and proximately causing the Equifax Data Breach; and

g. Violating the Oregon Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*, as alleged in more detail *infra*.

195. As a direct and proximate result of Equifax's practices, Oregon Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

196. The above unfair and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Oregon Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

197. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Oregon Subclass Members'

198. Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

199. Plaintiff and Oregon Subclass Members seek all remedies available under Or. Rev. Stat. § 646.638, including equitable relief, actual damages, statutory damages of \$200 per violation, and/or punitive damages.

200. Plaintiff and Oregon Subclass Members also seek reasonable attorneys' fees and costs under Or. Rev. Stat. § 646.638(3).

PENNSYLVANIA

FORTY-EIGHTH CAUSE OF ACTION

**PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER
PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*
(Asserted by the Pennsylvania Subclass)**

201. Plaintiff Mercedes Pillette ("Plaintiff," for purposes of this Count), individually and on behalf of the other Pennsylvania Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

202. Plaintiff and Pennsylvania Subclass Members purchased goods and services from Equifax in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2, for personal, family, and/or household purposes.

203. Equifax operating in Pennsylvania engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the

services purchased by the Pennsylvania Subclass in violation of 73 Pa. Cons. Stat. § 201-3, including but not limited to the following:

- a. Misrepresenting material facts pertaining to the sale of its goods and services to the Pennsylvania Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Pennsylvania Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of 73 Pa. Cons. Stat. §§ 201-3(4)(v), (vii), (ix), and (xxi);
- b. Misrepresenting material facts pertaining to the sale of its goods and services to Pennsylvania Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Pennsylvania Subclass Members' Personal Information in violation of 73 Pa. Cons. Stat. §§ 201-3(4) (v), (vii), (ix), and (xxi);
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Pennsylvania Subclass Members' Personal Information in violation of in violation of 73 Pa. Cons. Stat. §§ 201-3(4)(v), (vii), (ix), and (xxi);;

d. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of Pennsylvania Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Pennsylvania Subclass Members in a timely and accurate manner, in violation of 73 Pa. Cons. Stat. § 2303(a); and

f. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Pennsylvania Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

204. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Pennsylvania Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

205. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Pennsylvania Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Pennsylvania Subclass.

206. As a direct and proximate result of Equifax's deceptive acts and practices, Pennsylvania Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

207. Plaintiff and Pennsylvania Subclass Members seek relief under 73 Pa. Cons. Stat. § 201-9.2, including, but not limited to, injunctive relief, actual

damages or \$100 per Subclass Member, whichever is greater, treble damages, and attorneys' fees and costs.

RHODE ISLAND

FORTY-NINTH CAUSE OF ACTION

**RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT,
R.I. Gen. Laws §§ 6-13.1, *et seq.*
(Asserted by the Rhode Island Subclass)**

208. Plaintiff Darlene Brown ("Plaintiff," for purposes of this Count), individually and on behalf of the other Rhode Island Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

209. Plaintiff and Rhode Island Subclass Members purchased goods and services from Equifax in "trade" and "commerce," as meant by R.I. Gen. Laws § 6-13.1-1, for personal, family, and/or household purposes.

210. Equifax operating in Rhode Island engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Rhode Island Subclass in violation of R.I. Gen. Laws § 6-13.1-2, including but not limited to the following:

- a. Misrepresenting material facts pertaining to the sale of its goods and services to Rhode Island Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Rhode Island Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of R.I. Gen. Laws §§ 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);
- b. Misrepresenting material facts pertaining to the sale of its goods and services to Rhode Island Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Rhode Island Subclass Members' Personal Information in violation of R.I. Gen. Laws §§ 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Rhode Island Subclass Members' Personal Information in violation of in violation of R.I. Gen. Laws §§ 6- 13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);
- d. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of its goods and services by failing to maintain

the privacy and security of Rhode Island Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, and Rhode Island's data breach statute (R.I. Gen. Laws § 11-49.2-2(2));

e. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of its goods and services by failing to disclose the Equifax Data Breach to Rhode Island Subclass Members in a timely and accurate manner, in violation of R.I. Gen. Laws § 11-49.2-3(a); and

f. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of its goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Rhode Island Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

211. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Rhode Island Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

212. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Rhode Island Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Rhode Island Subclass.

213. As a direct and proximate result of Equifax's deceptive acts and practices, Rhode Island Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

214. Plaintiff and Rhode Island Subclass Members seek relief under R.I. Gen. Laws § 6-13.1-5.2, including, but not limited to, injunctive relief, other

equitable relief, actual damages or \$200 per Subclass Member, whichever is greater, punitive damages, and attorneys' fees and costs.

SOUTH CAROLINA

FIFTIETH CAUSE OF ACTION

**SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT,
S.C. Code Ann. §§ 39-5-10, *et seq.*
(Asserted by the South Carolina Subclass)**

215. Plaintiff Craig Maxwell ("Plaintiff," for purposes of this Count), individually and on behalf of the other South Carolina Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

216. Equifax is a "person" under S.C. Code Ann. § 39-5-10.

217. The South Carolina Unfair Trade Practices Act prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce" S.C. Code Ann. § 39-5-20(a). Equifax's actions as set herein occurred in the conduct of trade or commerce.

218. Equifax operating in South Carolina willfully failed to disclose and actively concealed its inadequate computer and data security, the fact that it had suffered numerous data breaches, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or

concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its provision of credit bureau services.

219. Equifax knew it had taken inadequate measures to ensure the security and integrity of its computer and data systems and it knew it had suffered numerous data breaches. Equifax knew this for at least several months, but concealed all of that information.

220. By failing to disclose that its computer and data security measures were inadequate and that it had suffered numerous data breaches, Equifax engaged in deceptive business practices.

221. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and South Carolina Subclass Members, about the inadequacy of Equifax's computer and data security and the quality of the Equifax brand.

222. Equifax intentionally and knowingly misrepresented material facts regarding the security and integrity of its computer and data systems with an intent to mislead Plaintiff and the South Carolina Subclass.

223. Equifax knew or should have known that its conduct violated the South Carolina Unfair Trade Practices Act.

224. As alleged above, Equifax made material statements about the security and integrity of its computer and data systems and the Equifax brand that were either false or misleading.

225. Equifax owed Plaintiff and the South Carolina Subclass a duty to disclose the true nature of its computer and data systems because Equifax:

- a. Possessed exclusive knowledge regarding the security of consumers' data;
- b. Intentionally concealed the foregoing from Plaintiff and the South Carolina Subclass; and/or
- c. Made incomplete representations about the security and integrity of its computer and data systems generally, and its prior data breaches in particular, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

226. Equifax's fraudulent claims of data and computer security and the true nature of its computer and data system security were material to Plaintiff and the South Carolina Subclass.

227. Plaintiff and the South Carolina Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information.

228. Plaintiff and South Carolina Subclass Members Personal Information would not have been stolen but for Equifax's actions and inactions.

229. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices. Plaintiff and the South Carolina Subclass Members suffered ascertainable loss in the form of the theft of their Personal Information as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

230. Equifax's violations present a continuing risk to Plaintiff and South Carolina Subclass Members as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest. As a direct and proximate result of Equifax's actions and inactions, Plaintiff and South Carolina Subclass Members have suffered injury-in-fact and/or actual damage.

231. Pursuant to S.C. Code Ann. § 39-5-140(a), Plaintiff and South Carolina Subclass Members seek monetary relief against Equifax to recover for their economic losses. Because Equifax's actions were willful and knowing, Plaintiff and South Carolina Subclass Members' damages should be trebled.

232. Plaintiff and South Carolina Subclass Members further allege that Equifax's malicious and deliberate conduct warrants an assessment of punitive damages because Equifax carried out despicable conduct with willful and conscious disregard of the rights and safety of others, subjecting Plaintiff and South Carolina Subclass Members to unjust hardship as a result. Equifax's intentionally and willfully misrepresented the security and integrity of its computer and data systems, deceived Plaintiff and the South Carolina Subclass, and concealed material facts that only Equifax knew. Equifax's unlawful conduct constitutes malice, oppression, and fraud warranting punitive damages.

233. Plaintiff and South Carolina Subclass Members further seek an order enjoining Equifax's unfair and deceptive acts and practices.

SOUTH DAKOTA

FIFTY-FIRST CAUSE OF ACTION

SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT, S.D. Codified Laws §§ 37-24-1, *et seq.* (Asserted by the South Dakota Subclass)

234. Plaintiff Kody Campbell ("Plaintiff," for purposes of this Count), individually and on behalf of the other South Dakota Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

235. Equifax advertises and sells “goods or services” and/or “merchandise” in “trade” and “commerce,” as meant by S.D. Codified Laws § 37-24-1, in the form of goods and services.

236. Equifax operating in South Dakota engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of S.D. Codified Laws § 37-24-6, including but not limited to the following:

- a. Knowingly and intentionally misrepresenting material facts, pertaining to the sale of goods and services, to the South Dakota Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard South Dakota Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of S.D. Codified Laws § 37-24-6(1);
- b. Knowingly and intentionally misrepresenting material facts, pertaining to the sale of goods and services, to the South Dakota Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the

privacy and security of South Dakota Subclass Members' Personal Information in violation of S.D. Codified Laws § 37-24-6(1);

c. Knowingly and intentionally omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for South Dakota Subclass Members' Personal Information in violation of S.D. Codified Laws § 37-24-6(1);

d. Engaging in deceptive acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of South Dakota Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Knowingly and intentionally engaging in deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to South Dakota Subclass Members in a timely and accurate manner; and

f. Engaging in deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect South Dakota Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

237. The above deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and South Dakota Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

238. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard South Dakota Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the South Dakota Subclass.

239. As a direct and proximate result of Equifax's deceptive acts and practices, South Dakota Subclass Members were adversely affected, injured, and/or damaged.

240. Plaintiff and South Dakota Subclass Members seek relief under S.D. Codified Laws § 37-24-31, including, but not limited to, actual damages.

TENNESSEE

FIFTY-SECOND CAUSE OF ACTION

**TENNESSEE CONSUMER PROTECTION ACT,
Tenn. Code Ann. §§ 47-18-101, *et seq.*
(Asserted by the Tennessee Subclass)**

241. Plaintiff Mildred Sutton (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Tennessee Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

242. Equifax advertised and sold “goods” or “services” in “trade” and “commerce,” as meant by Tenn. Code § 47-18-103.

243. Equifax operating in Tennessee engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of Tenn. Code Ann. § 47-18-104, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of goods and services, to the Tennessee Subclass by representing that it would maintain adequate data privacy and security practices and procedures

to safeguard Tennessee Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Tenn. Code Ann. §§ 47-18-104(b)(5), (7), and (9);

b. Misrepresenting material facts, pertaining to the sale of goods and services, to Tennessee Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Tennessee Subclass Members' Personal Information in violation of Tenn. Code Ann. §§ 47-18-104(b)(5), (7) and (9);

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Tennessee Subclass Members' Personal Information in violation of Tenn. Code Ann. §§ 47-18-104(b)(5), (7), and (9);

d. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of Tennessee Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax

Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to Tennessee Subclass Members in a timely and accurate manner, in violation of Tenn. Code Ann. § 47-18-2107(b); and

f. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Tennessee Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

244. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Tennessee Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

245. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Tennessee Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Tennessee Subclass.

246. As a direct and proximate result of Equifax's deceptive acts and practices, the Tennessee Subclass Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their

247. legally protected interest in the confidentiality and privacy of their Personal Information.

248. Plaintiff and Tennessee Subclass Members seek relief under Tenn. Code Ann. § 47-18-109, including, but not limited to, injunctive relief, actual damages, treble damages for each willful or knowing violation, and attorneys' fees and costs.

UTAH

FIFTY-THIRD CAUSE OF ACTION

**UTAH CONSUMER SALES PRACTICES ACT,
Utah Code §§ 13-11-1, *et seq.*
(Asserted by the Utah Subclass)**

249. Plaintiff Abby Elliott, (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Utah Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

250. The actions described above involved “consumer transactions” within the meaning of Utah Code § 13-11-1(2).

251. Equifax is a “supplier” within the meaning of Utah Code § 13-11-1(6).

252. Equifax operating in Utah engaged in deceptive trade practices in connection with consumer transactions, including by representing that its goods and services had characteristics that they did not have and representing that its services were of a particular standard or quality when they were not, in violation of Utah Code § 13-11-4. This includes but is not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect Utah Subclass Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;

- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard Utah Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for Utah Subclass Members' Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Utah Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA; and
- f. Failing to maintain the privacy and security of Utah Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those

mentioned in the aforementioned paragraph, directly and proximately causing the Equifax Data Breach.

253. As a direct and proximate result of Equifax's practices, Utah Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

254. The above unfair and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Utah Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

255. The above acts were also unconscionable acts or practices by a supplier in violation of Utah Code § 13-11-5.

256. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Utah Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

257. Plaintiff and Utah Subclass Members seek all available relief under Utah Code §§ 13-11-1, *et seq.*, including, but not limited to, actual damages, civil penalties, injunctive relief, and attorneys’ fees and costs.

VERMONT

FIFTY-FOURTH CAUSE OF ACTION

**VERMONT CONSUMER FRAUD ACT,
Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*
(Asserted by the Vermont Subclass)**

258. Plaintiff Jennifer Wise (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Vermont Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

259. Plaintiff and Vermont Subclass Members are “consumers” as meant by Vt. Stat. Ann. tit. 9, § 2451a.

260. Plaintiff and Vermont Subclass Members purchased “goods” or “services,” as meant by Vt. Stat. Ann. tit. 9, § 2451a, for personal, family, and/or household purposes.

261. Equifax operating in Vermont engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods

and services in violation of Vt. Stat. Ann. tit. 9, § 2453, including but not limited to the following:

- a. Misrepresenting material facts pertaining to the sale of goods and services to Vermont Subclass Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Vermont Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts pertaining to the sale of goods and services to Vermont Subclass Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Vermont Subclass Members' Personal Information;
- c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Vermont Subclass Members' Personal Information;
- d. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of Vermont Subclass Members' Personal

Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA and the GLBA;

e. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Equifax Data Breach to Vermont Subclass Members in a timely and accurate manner, in violation of 9 Vt. Stat. Ann. § 2435(b)(1); and

f. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods and services by failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Vermont Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

262. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Vermont Subclass Members that they could not

reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

263. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Vermont Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Vermont Subclass.

264. As a direct and proximate result of Equifax's deceptive acts and practices, Vermont Subclass Members suffered injury and/or damages.

265. Plaintiff and Vermont Subclass Members seek relief under Vt. Stat. Ann. tit. 9, § 2461, including, but not limited to, injunctive relief, restitution, actual damages, disgorgement of profits, exemplary damages, and attorneys' fees and costs.

VIRGINIA

FIFTY-FIFTH CAUSE OF ACTION

**VIRGINIA CONSUMER PROTECTION ACT,
Va. Code Ann. §§ 59.1-196, *et seq.*
(Asserted by the Virginia Subclass)**

266. Plaintiff Bridget Craney (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Virginia Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

267. The Virginia Consumer Protection Act prohibits “[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.” Va. Code Ann. § 59.1-200(14).

268. Equifax compiled, maintained, used, and furnished Plaintiff’s and Virginia Subclass Members’ Personal Information in connection with consumer transactions, as defined under Va. Code Ann. § 59.1-198, including, for example, credit assessments.

269. Equifax operating in Virginia engaged in deceptive trade practices in connection with consumer transactions, including by representing that its goods and services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised, in violation of Va. Code Ann. § 59.1-200. This includes but is not limited to the following:

- a. Failing to enact adequate privacy and security measures to protect Virginia Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax Data Breach;
- b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;
- c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard Virginia Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for Virginia Subclass Members' Personal Information;
- e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Virginia Subclass Members' Personal Information, including but not limited to duties imposed by the FCRA and the GLBA; and

f. Failing to maintain the privacy and security of Virginia Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Equifax Data Breach.

270. As a direct and proximate result of Equifax's practices, Virginia Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

271. The above unfair and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Virginia Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

272. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Virginia Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

273. Plaintiff and Virginia Subclass Members seek all available relief under Va. Code Ann. § 59.1-204, including, but not limited to, actual damages, statutory damages and/or penalties in the amount of \$1,000 per violation or, in the alternative, \$500 per violation, restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

WASHINGTON

FIFTY-SIXTH CAUSE OF ACTION

**WASHINGTON CONSUMER PROTECTION ACT,
Wash. Rev. Code Ann. §§ 19.86.020, *et seq.*
(Asserted by the Washington Subclass)**

274. Plaintiff Robert Wickens ("Plaintiff," for purposes of this Count), individually and on behalf of the other Washington Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

275. Equifax operating in Washington engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including but not limited to the following:

- a. Misrepresenting and fraudulently advertising material facts pertaining to the sale of its goods and services to Washington Subclass Members by representing and advertising that it would maintain adequate data privacy and security practices and procedures

to safeguard Washington Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts pertaining to goods and services to the Washington Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state

c. laws pertaining to the privacy and security of Washington Subclass Members' Personal Information;

d. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Washington Subclass Members' Personal Information;

e. Engaging in deceptive, unfair and unlawful trade acts or practices by failing to maintain the privacy and security of Washington Subclass Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Equifax Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FRCA, the GLBA, and the Washington regulations pertaining to Privacy of Consumer Financial and Health Information (Wash. ADC 284-04-300);

f. Failing to disclose the Equifax Data Breach to Washington Subclass Members in a timely and accurate manner, contrary to the duties imposed by Wash. Rev. Code Ann. § 19.255.010(1); and

g. Failing to take proper action following the Equifax Data Breach to enact adequate privacy and security measures and protect Washington Subclass Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

276. As a direct and proximate result of Equifax's deceptive trade practices, Washington Subclass Members suffered injury and/or damages.

277. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

278. injury to Plaintiff and Washington Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

279. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Washington Subclass Members' Personal Information and that risk of a data breach or theft was high. Equifax's actions in engaging in the above-named unfair practices and deceptive

280. acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Washington Subclass.

281. Plaintiff and Washington Subclass Members seek relief under Wash. Rev. Code Ann. § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

WISCONSIN

FIFTY-SEVENTH CAUSE OF ACTION

**WISCONSIN DECEPTIVE TRADE PRACTICES ACT,
Wis. Stat. § 100.18
(Asserted By The Wisconsin Subclass)**

282. Plaintiff Kyle Olson ("Plaintiff," for purposes of this Count), individually and on behalf of the other Wisconsin Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

283. Equifax is a "person, firm, corporation or association" within the meaning of Wis. Stat. § 100.18(1).

284. Plaintiff and Wisconsin Subclass Members are members of "the public" within the meaning of Wis. Stat. § 100.18(1).

285. Plaintiff and Wisconsin Subclass Members were deceived as described herein and have suffered damages as a result.

286. Equifax operating in Wisconsin willfully failed to disclose and actively concealed its inadequate computer and data security discussed herein and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its provision of credit bureau services.

287. By failing to disclose that its computer and data systems were inadequately secured as described herein, Equifax engaged in deceptive business practices in violation of Wis. Stat. § 100.18.

288. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and Wisconsin Subclass

289. Members, about the true nature of its computer and data security and the quality of the Equifax brand.

290. Equifax intentionally and knowingly misrepresented material facts regarding the security and integrity of its computer and data systems with an intent to mislead Plaintiff and Wisconsin Subclass Members.

291. Equifax knew or should have known that its conduct violated Wis. Stat. § 100.18.

292. As alleged above, Equifax made material statements about the security and integrity of its computer and data systems, and the Equifax brand that were either false or misleading.

293. Equifax owed Plaintiff and Wisconsin Subclass Members a duty to disclose the true nature of the security of its computer and data systems, because Equifax:

- a. Possessed exclusive knowledge regarding the lack of security of consumers' information, and that it had suffered data breaches;
- b. Intentionally concealed the foregoing from Plaintiff and Wisconsin Subclass Members; and/or
- c. Made incomplete representations about the security and integrity of its computer and data systems generally, and its prior data breaches in particular, while purposefully withholding material facts from Plaintiff and Wisconsin Subclass Members that contradicted these representations.

294. Equifax's fraudulent claims of computer and data security and the true nature of the security of such systems were material to Plaintiff and Wisconsin Subclass Members.

295. Plaintiff and Wisconsin Subclass Members suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Subclass Members would not have had their Personal Information stolen and would have taken steps to prevent identity theft and other harms, but for Equifax's violations described herein.

296. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under Wis. Stat. § 100.18.

297. All Wisconsin Subclass Members suffered ascertainable loss, including in the form of out of pocket expenses and lost time to implement and maintain credit freezes and identity theft prevention as a result of Equifax's deceptive and unfair acts and practices made in the course of its business. Equifax's violations present a continuing risk to Plaintiff and Wisconsin Subclass Members as well as to the general public.

298. Equifax's unlawful acts and practices complained of herein affect the public interest.

299. As a direct and proximate result of Equifax's violations of Wis. Stat. § 100.18, Plaintiff and Wisconsin Subclass Members have suffered injury-in fact and/or actual damage.

300. Plaintiff and Wisconsin Subclass Members are entitled to damages and other relief provided for under Wis. Stat. § 100.18(11)(b)(2).

301. Because Equifax's conduct was committed knowingly and/or intentionally, Plaintiff and Wisconsin Subclass Members are entitled to treble damages.

302. Plaintiff and Wisconsin Subclass Members also seek court costs and attorneys' fees under Wis. Stat. § 100.18(11)(b)(2).

FIFTY-EIGHTH CAUSE OF ACTION

WYOMIN CONSUMER PROTECTION ACT

Wyo. Stat. Ann. §§ 40-12-101, *et seq.*

(Asserted by the Wyoming Subclass)

303. Plaintiff Mel Orchard III ("Plaintiff," for purposes of this Count), individually and on behalf of the other Wyoming Subclass members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

304. Equifax is a "person" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(i).

305. Equifax's goods and services are "merchandise" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(vi).

306. Equifax has "advertised" its goods and services within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(v).

307. Plaintiff sent a demand for relief on behalf of the Wyoming Subclass pursuant to Wyo. Stat. Ann. § 40-12-109 on October 10, 2017.

308. Equifax operating in Wyoming engaged in deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Wyoming Subclass Members in violation of Wyo. Stat. Ann. § 40-12-105, including but not limited to the following:

- a. Representing that merchandise has a source, origin, sponsorship, approval, accessories or uses it does not have;
- b. Representing that merchandise is of a particular standing, grade, style or model when it is not;
- c. Advertising merchandise with intent not to sell it as advertised;
and
- d. Engaging in unfair or deceptive acts or practices.

309. Equifax knew, or in the exercise of due care should have known, that it has in the past or is so representing to Wyoming Subclass Members regarding its data privacy and security practices was untrue.

310. Wyoming Subclass Members have suffered actual damages as a result of Equifax's unfair or deceptive acts or practices.

311. Equifax's conduct proximately caused the injuries to Plaintiff and the Wyoming Subclass Members.

312. Pursuant to Wyo. Stat. Ann. §§ 40-12-108 & 208, Plaintiff asks the Court to enter injunctive relief to require Equifax to stop the unfair and deceptive conduct alleged herein, to assess damages to be proven at trial, costs, and attorneys' fees, and to award punitive damages against Equifax for its unlawful acts and trade practices.

VIII. STATE DATA BREACH STATUTES BROUGHT BY THE STATEWIDE SUBCLASSES BELOW

ALASKA

FIFTY-NINTH CAUSE OF ACTION

PERSONAL INFORMATION PROTECTION ACT,

Alaska Stat. §§ 45.48.010, *et seq.*

(Asserted by the Alaska Subclass)

313. Plaintiff Michael Bishop (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Alaska Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

314. Equifax is required to accurately notify Plaintiff and Alaska Subclass Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Alaska Stat. § 45.48.010.

315. Equifax is similarly required to determine the scope of the breach and restore the reasonable integrity of the information system under Alaska Stat. § 45.48.010.

316. Equifax is a business that owns or licenses personal information as defined by Alaska Stat. § 45.48.010.

317. Plaintiff and Alaska Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Alaska Stat. § 45.48.010.

318. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Alaska Stat. § 45.48.010.

319. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner Equifax violated Alaska Stat. § 45.48.010.

320. As a direct and proximate result of Equifax's violations of Alaska Stat. § 45.48.010, Plaintiff and Alaska Subclass Members suffered damages, as described above.

321. Plaintiff and Alaska Subclass Members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial, or (c) statutory damages in the amount of \$500 for Plaintiff and each Alaska Subclass Member; reasonable attorneys' fees; and any other just and proper relief available under Alaska Stat. § 45.48.010.

CALIFORNIA

SIXTIETH CAUSE OF ACTION

CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80, *et seq.* (Asserted by the California Subclass)

322. Plaintiff Miche' Sharpe ("Plaintiff," for purposes of this Count), individually and on behalf of the other California Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

323. “[T]o ensure that personal information about California residents is protected,” the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that “owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure herein.”

324. Equifax is a business that owns, maintains, and licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass Members.

325. Businesses that own or license computerized data that includes personal information, including Social Security numbers, are required to notify California residents when their Personal Information has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include “the types of personal information that were or are reasonably believed to have been the subject of the breach.: Cal. Civ. Code § 1798.82

326. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

327. Plaintiff and California Subclass Members' Personal Information (*e.g.*, Social Security numbers) includes personal information as covered by Cal. Civ. Code § 1798.82.

328. Because Equifax reasonably believed that Plaintiff's and California Subclass Members' Personal Information was acquired by unauthorized persons during the Equifax Data Breach, Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

329. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

330. As a direct and proximate result of Equifax's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members suffered damages, as described above.

331. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including, but not limited to, actual damages and injunctive relief.

COLORADO

SIXTY-FIRST CAUSE OF ACTION

**COLORADO SECURITY BREACH NOTIFICATION ACT,
Colo. Rev. Stat. Ann. §§ 6-1-716, *et seq.*
(Asserted by the Colorado Subclass)**

332. Plaintiff Gerald Muhammad (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Colorado Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

333. Equifax is required to accurately notify Plaintiff and Colorado Subclass Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. Ann. § 6- 1-716(2).

334. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Colo. Rev. Stat. Ann. §§ 6-1-716(1) and (2).

335. Plaintiff and Colorado Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered by Colo. Rev. Stat. Ann. §§ 6-1-716(1) and (2).

336. Because Equifax was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. Ann. § 6-1-716 (2).

337. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated Colo. Rev. Stat. Ann. § 6-1-716 (2).

338. As a direct and proximate result of Equifax's violations of Colo. Rev. Stat. Ann. § 6-1-716(2), Plaintiff and Colorado Subclass Members suffered damages, as described above.

339. Plaintiff and Colorado Subclass Members seek relief under Colo. Rev. Stat. Ann. § 6-1-716(4), including, but not limited to, actual damages and equitable relief.

DELAWARE

SIXTY-SECOND CAUSE OF ACTION

DELAWARE COMPUTER SECURITY BREACH ACT, 6 Del. Code Ann. §§ 12B-102, *et seq.* (Asserted by the Delaware Subclass)

340. Plaintiff Alexandra Santana ("Plaintiff," for purposes of this Count), individually and on behalf of the other Delaware Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

341. Equifax is required to accurately notify Plaintiff and Delaware Subclass Members if Equifax becomes aware of a breach of its data security system (which is reasonably likely to result in the misuse of a Delaware resident's personal information) in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

342. Equifax is a business that owns or licenses computerized data that includes personal information as defined by 6 Del. Code Ann. § 12B-102(a).

343. Plaintiff and Delaware Subclass Members' Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under 6 Del. Code Ann. § 12B-101(4).

344. Because Equifax was aware of a breach of its security system (which is reasonably likely to result in misuse of Delaware residents' personal information), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

345. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated 6 Del. Code Ann. § 12B-102(a).

346. As a direct and proximate result of Equifax's violations of 6 Del. Code Ann. § 12B-102(a), Plaintiff and Delaware Subclass Members suffered damages, as described above.

347. Plaintiff and Delaware Subclass Members seek relief under 6 Del. Code Ann. § 12B-104, including, but not limited to, actual damages and broad equitable relief.

DISTRICT OF COLUMBIA

SIXTY-THIRD CAUSE OF ACTION

**DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH
NOTIFICATION ACT,**

D.C. Code §§ 28-3851, *et seq.*

(Asserted by the District of Columbia Subclass)

348. Plaintiff Joseph Creed Kelly (“Plaintiff,” for purposes of this Count), individually and on behalf of the other District of Columbia Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

349. Equifax is required to accurately notify Plaintiff and District of Columbia Subclass Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

350. Equifax is a business that owns or licenses computerized data that includes personal information as defined by D.C. Code § 28-3852(a).

351. Plaintiff and District of Columbia Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under D.C. Code § 28-3851(3).

352. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

353. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner Equifax violated D.C. Code § 28-3852(a).

354. As a direct and proximate result of Equifax's violations of D.C. Code § 28-3852(a), Plaintiff and District of Columbia Subclass Members suffered damages, as described above.

355. Plaintiff and District of Columbia Subclass Members seek relief under D.C. Code § 28-3853(a), including, but not limited to, actual damages.

GEORGIA

SIXTY-FOURTH CAUSE OF ACTION

GEORGIA SECURITY BREACH NOTIFICATION ACT, Ga. Code Ann. §§ 10-1-912, *et seq.* (Asserted by the Georgia Subclass)

356. Plaintiff Robert Hunt ("Plaintiff," for purposes of this Count), individually and on behalf of the other Georgia Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

357. Equifax is required to accurately notify Plaintiff and Georgia Subclass Members if it becomes aware of a breach of its data security system (that was

reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass Members' Personal Information) in the most expedient time possible and without unreasonable delay under Ga. Code Ann. § 10-1-912(a).

358. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Ga. Code Ann. § 10-1-912(a).

359. Plaintiff and Georgia Subclass Members' Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Ga. Code Ann. § 10-1-912(a).

360. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass Members' Personal Information), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

361. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated Ga. Code Ann. § 10-1-912(a).

362. As a direct and proximate result of Equifax's violations of Ga. Code Ann. § 10-1-912(a), Plaintiff and Georgia Subclass Members suffered damages, as described above.

363. Plaintiff and Georgia Subclass Members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

HAWAII

SIXTY-FIFTH CAUSE OF ACTION

**HAWAII SECURITY BREACH NOTIFICATION ACT,
Haw. Rev. Stat. §§ 487N-1, *et seq.*
(Asserted by the Hawaii Subclass)**

364. Plaintiff Bruce Pascal (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Hawaii Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

365. Equifax is required to accurately notify Plaintiff and Hawaii Subclass Members if it becomes aware of a breach of its data security system without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

366. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Haw. Rev. Stat. § 487N-2(a).

367. Plaintiff and Hawaii Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Haw. Rev. Stat. § 487N-2(a).

368. Because Equifax was aware of a breach of its security system, it had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

369. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated Haw. Rev. Stat. § 487N-2(a).

370. As a direct and proximate result of Equifax's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass Members suffered damages, as described above.

371. Plaintiff and Hawaii Subclass Members seek relief under Haw. Rev. Stat. § 487N-3(b), including, but not limited to, actual damages.

IOWA

SIXTY-SIXTH CAUSE OF ACTION

PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, Iowa Code Ann. §§ 715C.2, *et seq.* (Asserted by the Iowa Subclass)

372. Plaintiff Glenntavius Nolan ("Plaintiff," for purposes of this Count), individually and on behalf of the other Iowa Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

373. Equifax is required to accurately notify Plaintiff and Iowa Subclass Members if it becomes aware of a breach of its data security system in the most

expeditious time possible and without unreasonable delay under Iowa Code Ann. § 715C.2(1).

374. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Iowa Code Ann. § 715C.2(1).

375. Plaintiff's and Iowa Subclass Members' Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Iowa Code Ann. § 715C.2(1).

376. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code Ann. § 715C.2(1).

377. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated Iowa Code Ann. § 715C.2(1).

378. As a direct and proximate result of Equifax's violations of Iowa Code Ann. § 715C.2(1), Plaintiff and Iowa Subclass Members suffered damages, as above.

379. Plaintiff and Iowa Subclass Members seek relief under Iowa Code Ann. § 714.16(7), including, but not limited to, actual damages and injunctive relief.

KANSAS

SIXTY-SEVENTH CAUSE OF ACTION

**Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*
(Asserted by the Kansas Subclass)**

380. Plaintiff Amie Smith (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Kansas Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

381. Equifax is required to accurately notify Plaintiffs and Kansas Subclass Members if it becomes aware of a breach of its data security system (that was reasonably likely to have caused misuse of Plaintiff’s and Kansas Subclass Members’ Personal Information) in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

382. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Kan. Stat. Ann. § 50-7a02(a).

383. Plaintiff’s and Kansas Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Kan. Stat. Ann. § 50-7a02(a).

384. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused misuse of Plaintiffs’ and Kansas Subclass

Members' Personal Information), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

385. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated Kan. Stat. Ann. § 50-7a02(a).

386. As a direct and proximate result of Equifax's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass Members suffered damages, as described above.

387. Plaintiff and Kansas Subclass Members seek relief under Kan. Stat. Ann. § 50-7a02(g), including, but not limited to, broad equitable relief.

KENTUCKY

SIXTY-EIGHTH CAUSE OF ACTION

KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT, Ky. Rev. Stat. Ann. §§ 365.732, *et seq.* (Asserted by the Kentucky Subclass)

388. Plaintiff Mary Hexter Moneypenny ("Plaintiff," for purposes of this Count), individually and on behalf of the other Kentucky Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

389. Equifax is required to accurately notify Plaintiff and Kentucky Subclass Members if it becomes aware of a breach of its data security system (that

was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and the other Kentucky Subclass Members' Personal Information) in the most

390. expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

391. Equifax is a business that holds computerized data that includes personal information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

392. Plaintiff's and Kentucky Subclass Members' Personal Information includes personal information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

393. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass Members' Personal Information), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

394. Thus, by failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated Ky. Rev. Stat. Ann. § 365.732(2).

395. As a direct and proximate result of Equifax's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass Members suffered damages, as described above.

396. Plaintiff and Kentucky Subclass Members seek relief under Ky. Rev. Stat. Ann. § 446.070, including, but not limited to, actual damages.

LOUISIANA

SIXTY-NINTH CAUSE OF ACTION

**La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*
(Asserted by the Louisiana Subclass)**

397. Plaintiff Jasmine Guess (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Louisiana Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

398. Equifax is required to accurately notify Plaintiff and Louisiana Subclass Members if it becomes aware of a breach of its data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff’s and Louisiana Subclass Members’ Personal Information) in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

399. Equifax is a business that owns or licenses computerized data that includes personal information as defined by La. Rev. Stat. Ann. § 51:3074(C).

400. Plaintiff’s and Louisiana Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under La. Rev. Stat. Ann. § 51:3074(C).

401. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass Members' Personal Information), Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

402. As a direct and proximate result of Equifax's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass Members suffered damages, as described above.

403. Plaintiff and Louisiana Subclass Members seek relief under La. Rev. Stat. Ann. § 51:3075, including, but not limited to, actual damages.

MARYLAND

SEVENTIETH CAUSE OF ACTION

MARYLAND PERSONAL INFORMATION PROTECTION ACT, Md. Comm. Code §§ 14-3501, *et seq.* (Asserted by the Maryland Subclass)

404. Plaintiff Lisa Tyree ("Plaintiff," for purposes of this Count), individually and on behalf of the other Maryland Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

405. Under Md. Comm. Code § 14-3503(a), "[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business

that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of personal information owned or licensed and the nature and size of the business and its operations.”

406. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

407. Plaintiff and Maryland Subclass Members are “individuals” and “customers” as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

408. Plaintiff’s and Maryland Subclass Members’ Personal Information includes personal information as covered under Md. Comm. Code § 14-3501(d).

409. Equifax did not maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

410. The Equifax Data Breach was a “breach of the security of a system” as defined by Md. Comm. Code § 14-3504(1).

411. Under Md. Comm. Code § 14-3504(b)(1), “[a] business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.”

412. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), “[i]f, after the investigation is concluded, the business determines that misuse of the individual’s personal information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach” and that notification “shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system.”

413. Because Equifax discovered a security breach and had notice of a security breach, Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

414. As a direct and proximate result of Equifax’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and Maryland Subclass Members suffered damages, as described above.

415. Plaintiff and Maryland Subclass Members seek relief under Md. Comm. Code § 14-350, including, but not limited to, actual damages.

SEVENTY-FIRST CAUSE OF ACTION

**MARYLAND’S SOCIAL SECURITY NUMBER PRIVACY ACT,
Md. Comm. Code §§ 14-3401, *et seq.*
(Asserted by the Maryland Subclass)**

416. Plaintiff Lisa Tyree (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Maryland Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

417. Equifax is a “person” as covered by Md. Comm. Code § 14-3402.

418. Plaintiff and Maryland Subclass Members are “individual[s]” covered by Md. Comm. Code § 14-3402.

419. Md. Comm. Code § 14-3402 prohibits a person from requiring an individual to transmit his/her Social Security number over the Internet unless the connection is secure or the individual’s Social Security number is encrypted, and from initiating the transmission of an individual’s Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

420. As described above, Equifax transmitted Plaintiff’s and Maryland Subclass Members’ Social Security numbers over the Internet on unsecure

connections and/or without encrypting the Social Security Numbers in violation of Md. Comm. Code § 14-3402.

421. As a direct and proximate result of Equifax's violations of Md. Comm. Code § 14-3402, Plaintiff and Maryland Subclass Members suffered damages, as described above.

422. Plaintiff and Maryland Subclass Members seek relief under Md. Comm. Code § 14-3402, including, but not limited to, actual damages.

MICHIGAN

SEVENTY-SECOND CAUSE OF ACTION

**MICHIGAN IDENTITY THEFT PROTECTION ACT,
Mich. Comp. Laws Ann. §§ 445.72, *et seq.*
(Asserted by the Michigan Subclass)**

423. Plaintiff Nicole Walker ("Plaintiff," for purposes of this Count), individually and on behalf of the other Michigan Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

424. Equifax is required to accurately notify Plaintiff and Michigan Subclass Members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

425. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

426. Plaintiff's and Michigan Subclass Members' Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

427. Because Equifax discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

428. As a direct and proximate result of Equifax's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass Members suffered damages, as described above.

429. Plaintiff and Michigan Subclass Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including, but not limited to, a civil fine.

NEW HAMPSHIRE

SEVENTY-THIRD CAUSE OF ACTION

**N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq.*
(Asserted by the New Hampshire Subclass)**

430. Plaintiff Andrew Sheppe (“Plaintiff,” for purposes of this Count), individually and on behalf of the other New Hampshire Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

431. Equifax is required to accurately notify Plaintiff and New Hampshire Subclass Members if Equifax becomes aware of a breach of its data security system (in which misuse of Personal Information has occurred or is reasonably likely to occur) as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

432. Equifax is a business that owns or licenses computerized data that includes personal information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

433. Plaintiff’s and New Hampshire Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

434. Because Equifax was aware of a security breach (in which misuse of Personal Information has occurred or is reasonably likely to occur), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

435. As a direct and proximate result of Equifax's violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass Members suffered damages, as described above.

436. Plaintiff and New Hampshire Subclass Members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including, but not limited to, actual damages and injunctive relief.

NEW JERSEY

SEVENTY-FOURTH CAUSE OF ACTION

**NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT,
N.J. Stat. Ann. §§ 56:8-163, *et seq.*
(Asserted by the New Jersey Subclass)**

437. Plaintiff Carlos Martinho ("Plaintiff," for purposes of this Count), individually and on behalf of the other New Jersey Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

438. Under N.J. Stat. Ann. § 56:8-163(b), “[a]ny business ... that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers ... of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.”

439. Equifax is a business that compiles or maintains computerized records that include personal information on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

440. Plaintiff’s and New Jersey Subclass Members’ Personal Information (including but not limited to names, addresses, and Social Security numbers) includes personal information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

441. Because Equifax discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

442. By failing to disclose the Equifax Data Breach in a timely and accurate manner, Equifax violated N.J. Stat. Ann. § 56:8-163(b).

443. As a direct and proximate result of Equifax's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass Members suffered the damages described above.

444. Plaintiff and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including but not limited to treble damages (to be proven at trial), attorneys' fees and costs, and injunctive relief.

NORTH CAROLINA

SEVENTY-FIFTH CAUSE OF ACTION

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. Gen. Stat. Art. 2A §§ 75-60, *et seq.* (Asserted by the North Carolina Subclass)

445. Plaintiff Nancy Dubin ("Plaintiff," for purposes of this Count), individually and on behalf of the other North Carolina Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

446. Equifax is a business that owns or licenses computerized data that includes personal information as defined by N.C. Gen. Stat. Art. 2A § 75-61(1).

447. Plaintiff and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. Art. 2A § 75-61(2).

448. Equifax is required to accurately notify Plaintiff and North Carolina Subclass Members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. Art. 2A § 75-65.

449. Plaintiff's and North Carolina Subclass Members' Personal Information includes personal information as covered under N.C. Gen. Stat. Art. 2A § 75-61(10).

450. Because Equifax discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. Art. 2A. § 75-65.

451. As a direct and proximate result of Equifax's violations of N.C. Gen. Stat. Art. 2A § 75-65, Plaintiff and North Carolina Subclass Members suffered damages, as above.

452. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. Art. 2A § 75-65, including, but not limited to, a civil fine.

OREGON

SEVENTY-SIXTH CAUSE OF ACTION

**OREGON CONSUMER IDENTITY THEFT PROTECTION ACT,
Or. Rev. Stat. Ann. §§ 646A.604(1), *et seq.*
(Asserted by the Oregon Subclass)**

453. Plaintiff Patricia Baxter (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Oregon Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

454. Pursuant to Or. Rev. Stat. Ann. § 646A.622(1), a business “that maintains records which contain personal information” of an Oregon resident “shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.”

455. Equifax is a business that maintains records which contain personal information, within the meaning of Or. Rev. Stat. Ann. § 646A.622(1), about Plaintiff and Oregon Subclass Members.

456. Equifax violated Or. Rev. Stat. Ann. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff’s and Oregon Subclass Members’ Personal Information.

457. Equifax is required to accurately notify Plaintiff and Oregon Subclass Members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. Ann. § 646A.604(1).

458. Equifax is a business that owns, maintains, or otherwise possesses data that includes consumers personal information as defined by Or. Rev. Stat. Ann. § 646A.604(1).

459. Plaintiff's and Oregon Subclass Members' Personal Information includes personal information as covered under Or. Rev. Stat. Ann. § 646A.604(1).

460. Because Equifax discovered a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. Ann. § 646A.604(1).

461. As a direct and proximate result of Equifax's violations of Or. Rev. Stat. Ann. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass Members suffered damages, as described above.

462. Plaintiff and Oregon Subclass Members seek relief under Or. Rev. Stat. § 646A.624(3), including, but not limited to, actual damages and injunctive relief.

SOUTH CAROLINA

SEVENTY-SEVENTH CAUSE OF ACTION

**SOUTH CAROLINA DATA BREACH SECURITY ACT,
S.C. Code Ann. §§ 39-1-90, *et seq.*
(Asserted by the South Carolina Subclass)**

463. Plaintiff Craig Maxwell (“Plaintiff,” for purposes of this Count), individually and on behalf of the other South Carolina Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

464. Equifax is required to accurately notify Plaintiff and South Carolina Subclass Members following discovery or notification of a breach of its data security system (if personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm) in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

465. Equifax is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

466. Plaintiff's and South Carolina Subclass Members' Personal Information (*e.g.*, Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

467. Because Equifax discovered a breach of its data security system (in which personal information that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm), Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

468. As a direct and proximate result of Equifax's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass Members suffered damages, as described above.

469. Plaintiff and South Carolina Subclass Members seek relief under S.C. Code Ann. § 39-1-90(G), including, but not limited to, actual damages and injunctive relief.

TENNESSEE

SEVENTY-EIGHTH CAUSE OF ACTION

**TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT,
Tenn. Code Ann. §§ 47-18-2107, *et seq.*
(Asserted by the Tennessee Subclass)**

470. Plaintiff Mildred Sutton (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Tennessee Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

471. Equifax is required to accurately notify Plaintiff and Tennessee Subclass Members following discovery or notification of a breach of its data security system (in which unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person) in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

472. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

473. Plaintiff’s and Tennessee Subclass Members’ Personal Information (*e.g.*, Social Security numbers) include personal information as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

474. Because Equifax discovered a breach of its security system (in which unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person), Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

475. As a direct and proximate result of Equifax's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass Members suffered damages, as described above.

476. Plaintiff and Tennessee Subclass Members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including, but not limited to, actual damages, injunctive relief, and treble damages.

VIRGINIA

SEVENTY-NINTH CAUSE OF ACTION

**VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT,
Va. Code. Ann. §§ 18.2-186.6, *et seq.*
(Asserted by the Virginia Subclass)**

477. Plaintiff Bridget Craney ("Plaintiff," for purposes of this Count), individually and on behalf of the other Virginia Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein..

478. Equifax is required to accurately notify Plaintiff and Virginia Subclass Members following discovery or notification of a breach of its data security system (if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

479. Equifax is an entity that owns or licenses computerized data that includes personal information as defined by Va. Code Ann. § 18.2-186.6(B).

480. Plaintiff's and Virginia Subclass Members' Personal Information includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

481. Because Equifax discovered a breach of its security system (in which unencrypted or unredacted personal information was or is reasonably believed to

482. have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

483. As a direct and proximate result of Equifax's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass Members suffered damages, as described above.

484. Plaintiff and Virginia Subclass Members seek relief under Va. Code Ann. § 18.2-186.6(I), including, but not limited to, actual damages.

WASHINGTON

EIGHTIETH CAUSE OF ACTION

**WASHINGTON DATA BREACH NOTICE ACT,
Wash. Rev. Code Ann. §§ 19.255.010, *et seq.*
(Asserted by the Washington Subclass)**

485. Plaintiff Robert Wickens (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Washington Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

486. Equifax is required to accurately notify Plaintiff and Washington Subclass Members following discovery or notification of the breach of its data security system (if personal information was, or is reasonably believed to have

487. been, acquired by an unauthorized person and the personal information was not secured) in the most expedient time possible and without unreasonable delay under Wash. Rev. Code Ann. § 19.255.010(1).

488. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.010(1).

489. Plaintiff’s and Washington Subclass Members’ Personal Information includes personal information as covered under Wash. Rev. Code Ann. § 19.255.010(5).

490. Because Equifax discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1).

491. As a direct and proximate result of Equifax's violations of Wash. Rev. Code Ann. § 19.255.010(1), Plaintiff and Washington Subclass Members suffered damages, as described above.

492. Plaintiff and Washington Subclass Members seek relief under Wash. Rev. Code Ann. §§ 19.255.010(10)(a) and 19.255.010(10)(b), including, but not limited to, actual damages and injunctive relief.

WISCONSIN

EIGHTY-FIRST CAUSE OF ACTION

Wis. Stat. Ann. §§ 134.98(2), *et seq.*
(ASSERTED BY THE WISCONSIN SUBCLASS)

493. Plaintiff Kyle Olson ("Plaintiff," for purposes of this Count), individually and on behalf of the other Wisconsin Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

494. Equifax is required to accurately notify Plaintiff and Wisconsin Subclass Members if it knows that personal information in its possession has been acquired by a person whom it has not authorized to acquire the personal information within a reasonable time under Wis. Stat. Ann. §§ 134.98(2)-(3)(a).

495. Equifax is a business that maintains or licenses personal information as defined by Wis. Stat. Ann. § 134.98(2).

496. Plaintiff's and Wisconsin Subclass Members' Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Wis. Stat. Ann. § 134.98(1)(b).

497. Because Equifax knew that personal information in its possession had been acquired by a person whom it has not authorized to acquire the personal information, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. Ann. § 134.98(2).

498. As a direct and proximate result of Equifax's violations of Wis. Stat. Ann. § 134.98(3)(a), Plaintiff and Wisconsin Subclass Members suffered damages, as described above.

499. Plaintiff and Wisconsin Subclass Members seek relief under Wis. Stat. Ann. § 134.98, including, but not limited to, actual damages and injunctive relief.

WYOMING

EIGHTY-SECOND CAUSE OF ACTION

**Wyo. Stat. Ann. §§ 40-12-502(A), *et seq.*
(Asserted by the Wyoming Subclass)**

500. Plaintiff Mel Orchard III (“Plaintiff,” for purposes of this Count), individually and on behalf of the other Wyoming Subclass Members, repeats and alleges Paragraphs 1-160, as if fully alleged herein.

501. Equifax is required to accurately notify Plaintiff and Wyoming Subclass Members when it becomes aware of a breach of its data security system (if the misuse of personal identifying information has occurred or is reasonably likely to occur) in the most expedient time possible and without unreasonable delay under Wyo. Stat. Ann. § 40-12-502(a).

502. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Wyo. Stat. Ann. § 40-12-502(a).

503. Plaintiff’s and Wyoming Subclass Members’ Personal Information (*e.g.*, Social Security numbers) includes personal information as covered under Wyo. Stat. Ann. § 40-12-502(a).

504. Because Equifax was aware of a breach of its data security system (in which the misuse of personal identifying information has occurred or is reasonably likely to occur), Equifax had an obligation to disclose the Equifax Data Breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

505. As a direct and proximate result of Equifax's violations of Wyo. Stat. Ann. § 40-12-502(a), Plaintiff and Wyoming Subclass Members suffered damages, as described above.

506. Plaintiff and Equifax Subclass Members seek relief under Wyo. Stat. Ann. § 40-12-502(f), including, but not limited to, actual damages and broad equitable relief.

EIGHTY-THIRD CAUSE OF ACTION

DECLARATORY AND INJUNCTIVE RELIEF

(Asserted by Plaintiffs, individually, and on behalf of the Nationwide class, and, in the alternative, Statewide Subclasses)

507. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this complaint.

508. An actual controversy has arisen in the wake of the Equifax Data Breach regarding its common law and other duties to reasonably safeguard its customers' PII and whether Equifax is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their personal information. Plaintiffs allege that Equifax's data security measures were and remain inadequate. Equifax denies these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

509. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Equifax owed and continues to owe a legal duty to secure consumers' personal and financial information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;
- b. Equifax continues to breach this legal duty by failing to employ reasonable measure to secure consumers' personal information/

510. The Court also should issue corresponding injunctive relief requiring

Equifax to employ adequate security protocols consistent with industry standards to protect consumers' personal and financial information.

511. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Equifax. The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

512. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another massive data breach occurs at Equifax, Plaintiffs will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

513. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Equifax, thus eliminating the additional injuries

that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class and Subclass Members, respectfully request that the Court enter judgment in their favor and against Equifax, as follows:

514. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' attorneys as Class Counsel;

515. That the Court grant permanent injunctive relief to prohibit Equifax from continuing to engage in the unlawful acts, omissions, and practices described herein;

516. That the Court award Plaintiffs and the other Class and Subclass Members compensatory, consequential, and general damages in an amount to be determined at trial;

517. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Equifax as a result of its unlawful acts, omissions, and practices;

518. That the Court award statutory damages, and punitive or exemplary damages, to the extent permitted by law;

519. That the unlawful acts alleged in this Complaint be adjudged and decreed to be unfair and deceptive business acts and practices in violation of the FCRA, state consumer protection laws, and state data breach laws;

520. That the unlawful acts alleged in this Complaint be adjudged and decreed to be negligence, negligence *per se*, bailment and unjust enrichment;

521. That Plaintiffs be granted the declaratory relief sought herein;

522. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, including fees and expenses;

523. That the Court award pre- and post-judgment interest at the maximum legal rate; and

That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: November 10, 2017

Respectfully submitted,

By: /s/ Kenneth S. Canfield

Kenneth S. Canfield

Georgia Bar No. 107744

DOFFERMYRE SHIELDS

CANFIELD & KNOWLES, LLC

1355 Peachtree St., NE, Suite 1600

Atlanta, Georgia 30309

Tel: (404) 881-8900

kcanfield@dsckd.com

Andrew N. Friedman (*Pro hac vice* to be submitted)

Douglas J. McNamara (*Pro hac vice* to be submitted)

Sally Handmaker (*Pro hac vice* to be submitted)

Eric S. Berelovich (*Pro hac vice* to be submitted)

COHEN MILSTEIN, SELLERS & TOLL PLLC

1100 New York Avenue, NW, Suite 500

Washington, DC 20005

Tel: (202) 408-4600

afriedman@cohenmilstein.com

dmcnamara@cohenmilstein.com

shandmaker@cohenmilstein.com

eberelovich@cohenmilstein.com

By: /s/ Roy E. Barnes

Roy E. Barnes

Georgia Bar No. 039000

John R. Bevis

Georgia Bar No. 056110

J. Cameron Tribble

Georgia Bar No. 754759

BARNES LAW GROUP, LLC

31 Atlanta Street

Marietta, GA 30060

Tel: (770) 227-6375

Fax: (770) 227-6373

roy@barneslawgroup.com

bevis@barneslawgroup.com

ctribble@barneslawgroup.com

Adam J. Levitt (*Pro hac vice* to be submitted)

Mark A. DiCello (*Pro hac vice* to be submitted)

Amy E. Keller (*Pro hac vice* to be submitted)

Daniel R. Ferri (*Pro hac vice* to be submitted)

DICELLO LEVITT & CASEY LLC

Ten North Dearborn Street, 11th Floor
Chicago, Illinois 60602

Tel: (312) 214-7900

alevitt@dlcfirm.com

madicello@dlcfirm.com

akeller@dlcfirm.com

dferri@dlcfirm.com

James Pizzirusso (*Pro hac vice* to be submitted)

HAUSFELD

1700 K St. NW, Suite 650

Washington, D.C. 20006

Tel: (202) 540-7200

jpizzirusso@hausfeld.com

Norman E. Siegel (*Pro hac vice* to be submitted)

Barrett J. Vahle (*Pro hac vice* to be submitted)

J. Austin Moore (*Pro hac vice* to be submitted)

STUEVE SIEGEL HANSON LLP

460 Nichols Road, Suite 200

Kansas City, Missouri 64112

Tel: (816) 714-7100

siegel@stuevesiegel.com

vahle@stuevesiegel.com

moore@stuevesiegel.com

John Yanchunis (*Pro hac vice* to be submitted)

Marisa Glassman (*Pro hac vice* to be submitted)

MORGAN & MORGAN

COMPLEX LITIGATION GROUP

201 North Franklin Street, 7th Floor

Tampa Florida 33602

Tel: (813) 223-5505

Fax: (813) 223-5402

jyanchunis@forthepeople.com

mglassman@forthepeople.com

Archie I. Grubb, II (*Pro hac vice* to be submitted)

W. Daniel “Dee” Miles, III (*Pro hac vice* to be submitted)

Andrew E. Brashier (*Pro hac vice* to be submitted)

Leslie Pescia (*Pro hac vice* to be submitted)

**BEASLEY, ALLEN, CROW,
METHVIN, PORTIS & MILES,
P.C.**

P.O. Box 4160

Montgomery, Alabama 36103

Tel: (334) 269-2343

Fax: (334) 954-7555

Archie.Grubb@BeasleyAllen.com

Dee.Miles@BeasleyAllen.com

Andrew.Brashier@BeasleyAllen.com

Leslie.Pescia@BeasleyAllen.com

Pat A. Cipollone, P.C. (*Pro hac vice* to be submitted)

Robert B. Gilmore (*Pro hac vice* to be submitted)

**STEIN MITCHELL CIPOLLONE
BEATO & MISSNER LLP**

1100 Connecticut Ave., N.W.

Washington, D.C. 20036

Tel: (202) 737-7777

pcipollone@steinmitchell.com

rgilmore@steinmitchell.com

*Counsel for Plaintiffs and the
Proposed Class and Subclass*